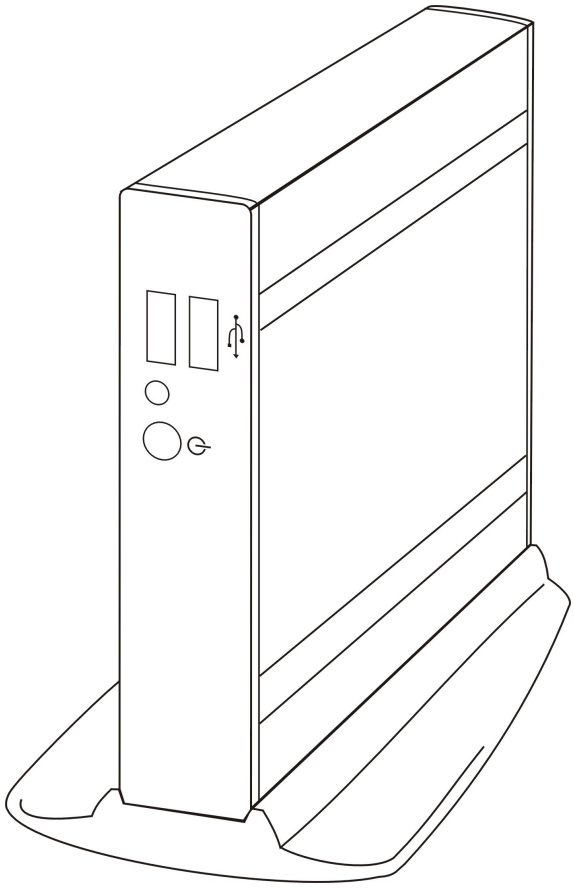
WML Linux Thin Client User Guide



Manual Version 1.1b

September 2008
WML Linux Thin Client User Guide
© 2008 William Matthew Limited. All rights reserved.
WML Linux Thin Client OS Release 2.5.1
All Trademarks observed.

Copyright © 2008 William Matthew Limited. All rights reserved

Acknowledgements: William Matthew Limited recognises and acknowledges all registered Trade Marks and copyright of all products mentioned within this guide.

E&OE

Software Licence and Copyright
The Software is copyright Embedded Software Foundry Limited. It is sold under licence by William Matthew Limited, 22 Haxey Lane, Haxey, Doncaster, South Yorkshire, DN9 2NE. UK. Email Info@wmltd.co.uk

"The Software" refers to the *Client Connection Manager* and the *Client Setup Manager*. The operating system source code is released under various free software licences, and may be obtained from William Matthew Limited on request.

IMPORTANT: Before using the Software installed on the WML Linux Thin Client please read the licence agreement carefully, the right to use this software is granted only if the Customer agrees to the terms of this Licence. If you do not agree to the terms of this Licence, please return the product unused.

Use of the Software is your acceptance of our terms and conditions of the license.

1. The Software has been developed for use with the WML Linux Thin Client Product range, The Licence is to be used without any time limit and maybe subject to change.

2. The Software may not be duplicated, copied, resold, or re-branded without the written consent of William Matthew Limited.

3. It is the responsibility of any user, reseller, Distributor, OEM and other third party to protect William Matthew Limited rights against violation of this Software Licence.

4. William Matthew will consider any attempt to duplicate the functionality of any application provided by the software will constitute a breach of software licence, and may instigate legal proceedings to protect the intellectual property rights of the WML Linux Thin Client and William Matthew Limited.

5. This Licence and the Software product may be transferred to a third party provided the third party agrees to all the terms of this licence and that no copies of the Software are retained by the transferring party.

6. William Matthew reserves the right to terminate this Licence upon breach.

7. In the event of a termination, all copies of the software must be returned to William Matthew Ltd

8. Any disputes In respect of the Software Licence will be considered a breach of copyright and is subject to English Law.

Copyright © 2008 William Matthew Limited. All rights reserved

Table of Contents

Introduction to WML Linux Thin Client....5
Technical Data....6
Connectivity Ports....6
Powering on/off....6
Monitors....6
Initial Setup Wizard....7
Client Connection Manager....12
Connections Tab – Overview....13
Configuration Tab – Overview....15
Creating a new Connection....16
Editing a Connection....18
NoMachine NX....18
Citrix ICA....18
NoMachine NX....19
NoMachine NX: Network Tab....19
Optional: NX key....20
NoMachine NX: Desktop Tab....21
Launching an NX Connection....22
Editing an existing NX connection....26
Citrix ICA....27
Sound support....27
Local USB storage device access....27
RDP: Remote Desktop Protocol....29
GraphOn GoGlobal For Windows....30
X Windows - XDMCP....32
XDMCP Broadcast....32
X Font Servers....33
VNC – TightVNC....34
Secure Shell - SSH....35
Telnet....36
Web Browser....37
Firefox settings....37
Custom programs....38
Sun Secure Global Desktop....39
Client Setup Manager....40
System....41
Saving and Loading System Settings....41
Restoring Factory Default Settings....43
Network-wide configuration....43
Locale....45
Network....46
Remote access to the WML Linux Thin Client....46
Remote SSH access....46
Remote VNC access....47
Specifying X Font Server (xfs)....47
Wireless networking....48
Display....51

Copyright © 2008 William Matthew Limited. All rights reserved

Mouse....52
Printing....53
Firmware....54
Manually Initiating a Firmware Upgrade....54
Automatic Firmware Upgrades....55
Installing a firmware upgrade file on a LAN web server....56
Password....58
Sound....59
Information....60
Administrator and Power User Tools....61
Startup script....61
Smartcard support....62

Copyright © 2008 William Matthew Limited. All rights reserved

Introduction to WML Linux Thin Client

The WML Linux Thin Client is a revolutionary Linux based thin client that allows easy windows style setup. The WML Linux Thin Client supports NoMachine NX, GraphOn GoGlobal for Windows, Citrix ICA client version 9, RDP5 connections, SSH (openssh), VNC (tightVNC) and X server (unix XDMCP).

The WML Linux Thin Client provides web browsing capabilities with Mozilla Firefox 1.5. Numerous embedded applications are provided for system admins and power users (scp, sftp, nano and vi).

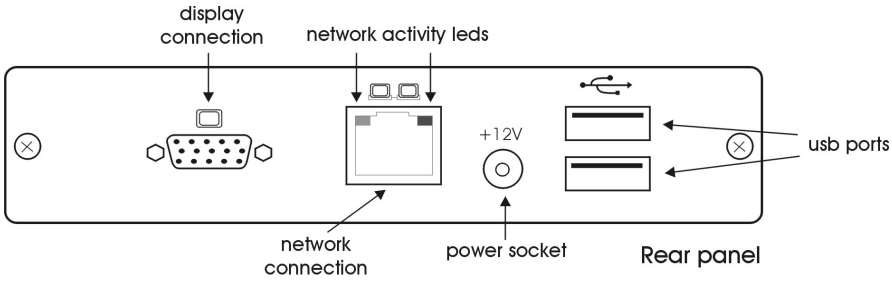
Based on the Sumo Technologies ST166 and ST168 hardware platforms, the WML Linux Thin Client will provide years of trouble free service.

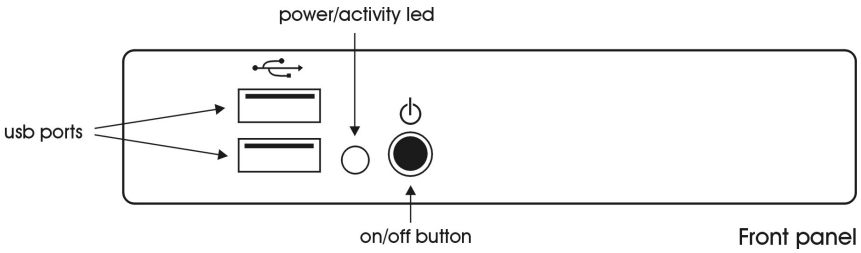
A unique feature of the WML Linux Thin Client is that programs normally associated with Windows based platforms can be embedded. The inclusion of the Mono runtime environment makes this possible. Mono is an implementation of the .NET1.1 framework. The WML Linux Thin Client provides Mono with Winforms and GTK#. These .NET applications can reside on a local webserver and the latest version of the application will be dynamically loaded on power up to every WML Linux Thin Client box on the network. This feature will allow you to centrally manage the software application and reduce the support required to maintain standard user desktops.

Copyright © 2008 William Matthew Limited. All rights reserved

Technical Data

Connectivity Ports





The unit comes with four USB V1.1 ports for this particular model. You can use one or all simultaneously for keyboard and mouse or other peripherals.

Powering on/off

The on/off button is the sole means for powering the unit on or off. When the on/off button is pressed while the unit is powered on, the WML Linux Thin Client will go into shutdown mode and will power off after about 3 seconds. If the unit fails to power off, hold the on/off button down for 10 seconds.

Monitors

The WML Linux Thin Client requires that the connected monitor provides the DDC protocol which allows the graphics software to determine the available resolution and frequency settings for the monitor. Most modern monitors are DDC compliant.

Copyright © 2008 William Matthew Limited. All rights reserved

Initial Setup Wizard

Connect a monitor to the unit's video port and a USB keyboard and mouse to any of the WML Linux Thin Client USB ports. The network connection should be connected to your LAN hub/switch or ADSL router using an RJ45 network cable.

Connect the supplied power adapter to the WML Linux Thin Client and press the on/off button and the blue led should illuminate and the unit should boot.

Note: USE ONLY THE SUPPLIED POWER ADAPTER OR YOU WILL INVALIDATE ANY WARRANTY.

The initial screen gives you the option of switching to your chosen locale. This will set the language and keyboard setting to match your country. If you change the locale, then the Setup Manager will re-start with the chosen keyboard and language.

Foundry Linux: Language and Locale
Language/Keyboard layout
Please choose your country. This will set the language and keyboard layout used in this wizard, the system setup window and the connection manager.
Please choose:
United Kingdom
Next

Illustration 1: Setup Wizard - Language and Keyboard Layout

Copyright © 2008 William Matthew Limited. All rights reserved

The second screen gives copyright information about the thin client.

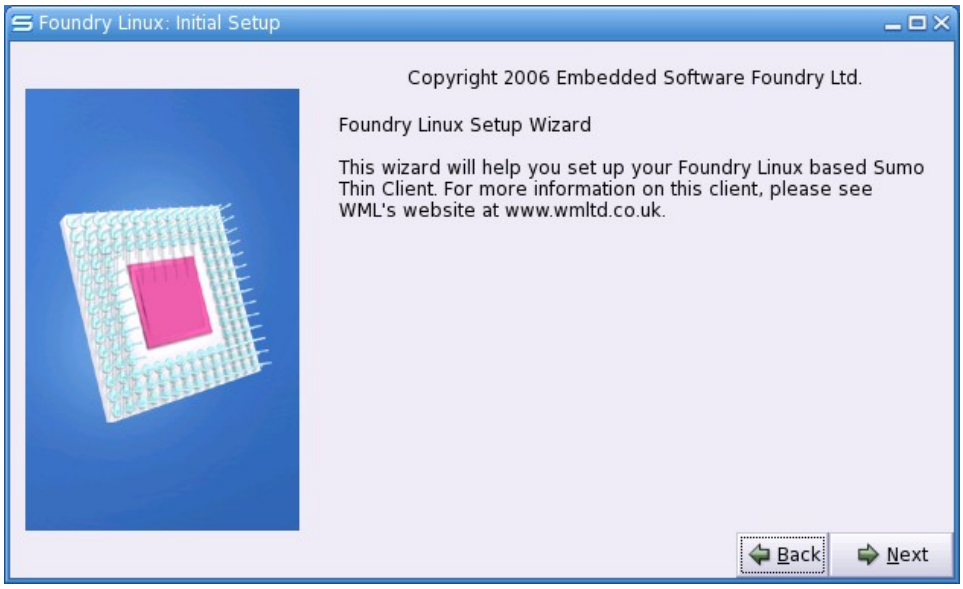

Foundry Linux: Initial Setup
Copyright 2006 Embedded Software Foundry Ltd.
Foundry Linux Setup Wizard
This wizard will help you set up your Foundry Linux based Sumo Thin Client. For more information on this client, please see WML's website at www.wmltd.co.uk.
Back
Next

Illustration 2: Setup Wizard - Initial Setup Window

The third screen gives you the choice of allowing DHCP to set the network settings for the client (selected by default) or configuring the settings manually.

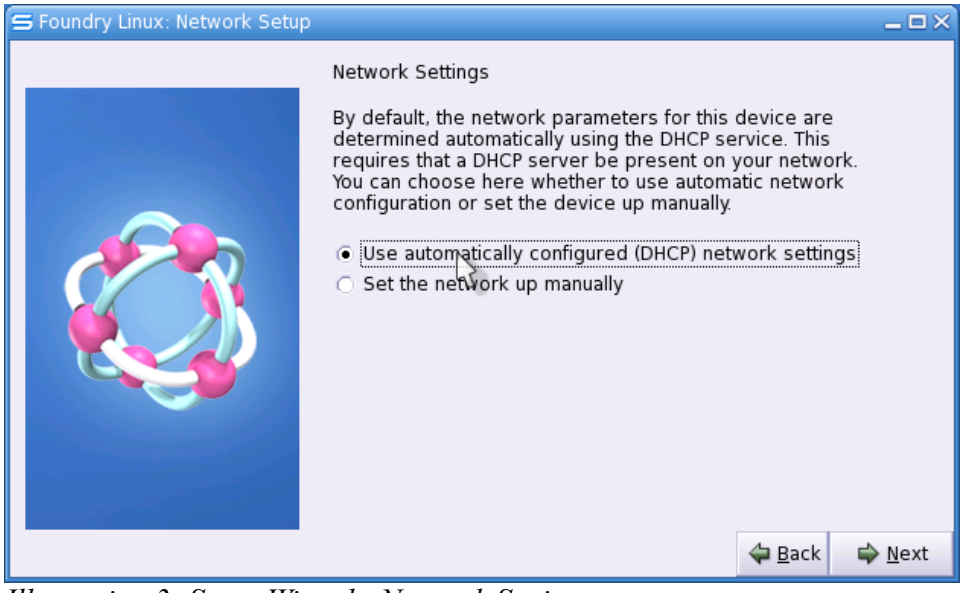

Foundry Linux: Network Setup
Network Settings
By default, the network parameters for this device are determined automatically using the DHCP service. This requires that a DHCP server be present on your network. You can choose here whether to use automatic network configuration or set the device up manually.
Use automatically configured (DHCP) network settings
Set the network up manually
Back
Next

Illustration 3: Setup Wizard - Network Settings

If "Set the network up manually" is chosen, you are presented with two screens to configure the IP address and the DNS settings.

Copyright © 2008 William Matthew Limited. All rights reserved

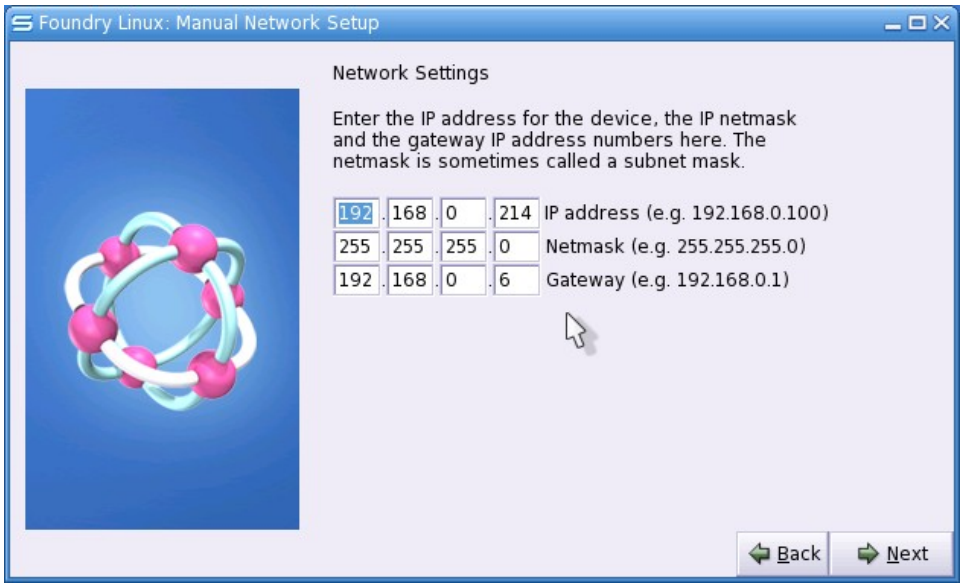

Foundry Linux: Manual Network Setup
Network Settings
Enter the IP address for the device, the IP netmask and the gateway IP address numbers here. The netmask is sometimes called a subnet mask.
192 . 168 . 0 . 214 IP address (e.g. 192.168.0.100)
255 . 255 . 255 . 0 Netmask (e.g. 255.255.255.0)
192 . 168 . 0 . 6 Gateway (e.g. 192.168.0.1)
Back
Next

Illustration 4: Setup Wizard - Manual IP Settings

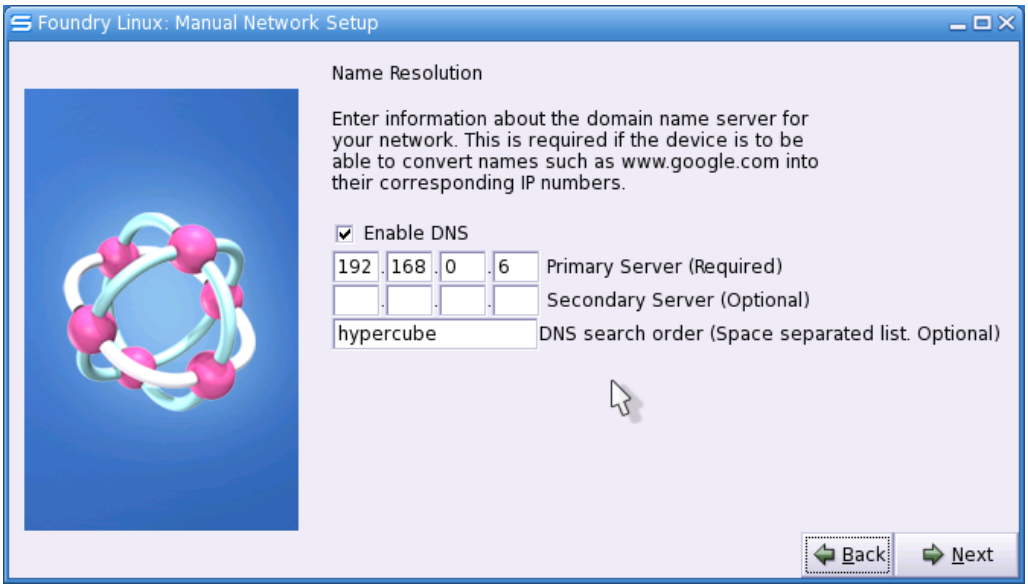

Foundry Linux: Manual Network Setup
Name Resolution
Enter information about the domain name server for your network. This is required if the device is to be able to convert names such as www.google.com into their corresponding IP numbers.
Enable DNS
192 . 168 . 0 . 6 Primary Server (Required)
Secondary Server (Optional)
hypercube DNS search order (Space separated list. Optional)
Back
Next

Illustration 5: Setup Wizard - Manual DNS Settings

After the network window(s) have been filled in, the network settings are applied.

Copyright © 2008 William Matthew Limited. All rights reserved

The next screen allows you to choose your preferred display resolution. The autodetected resolution will be shown pre-selected. If you change the resolution, the monitor will switch resolution and a confirmation window will appear. Click OK if the new resolution is functioning, or "Revert" to switch back to the original resolution. If the new resolution fails, and the display disappears, wait for 10 seconds, and the display will automatically revert back to the original autodetected resolution.

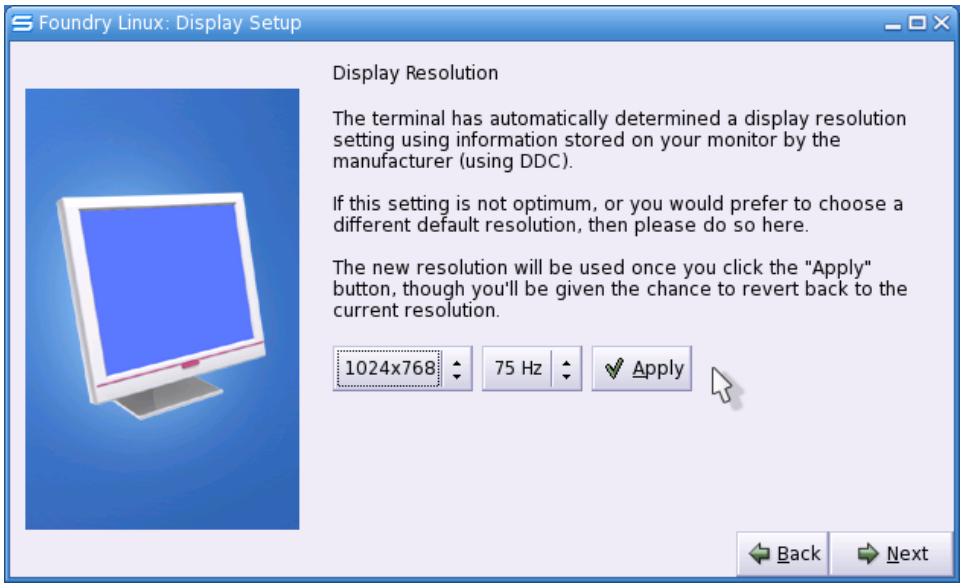

Foundry Linux: Display Setup
Display Resolution
The terminal has automatically determined a display resolution setting using information stored on your monitor by the manufacturer (using DDC).
If this setting is not optimum, or you would prefer to choose a different default resolution, then please do so here.
The new resolution will be used once you click the "Apply" button, though you'll be given the chance to revert back to the current resolution.
1024x768
75 Hz
Apply
Back
Next

Illustration 6: Setup Wizard - Display Resolution Settings

Printer setup will be displayed in the next window. If you require a locally connected printer on your WML Linux Thin Client, connect the printer to one of the USB ports. In order to print to the printer you will need to set up the print driver on a server and direct the print to the WML Linux Thin Client. An example of this process is described on this window.

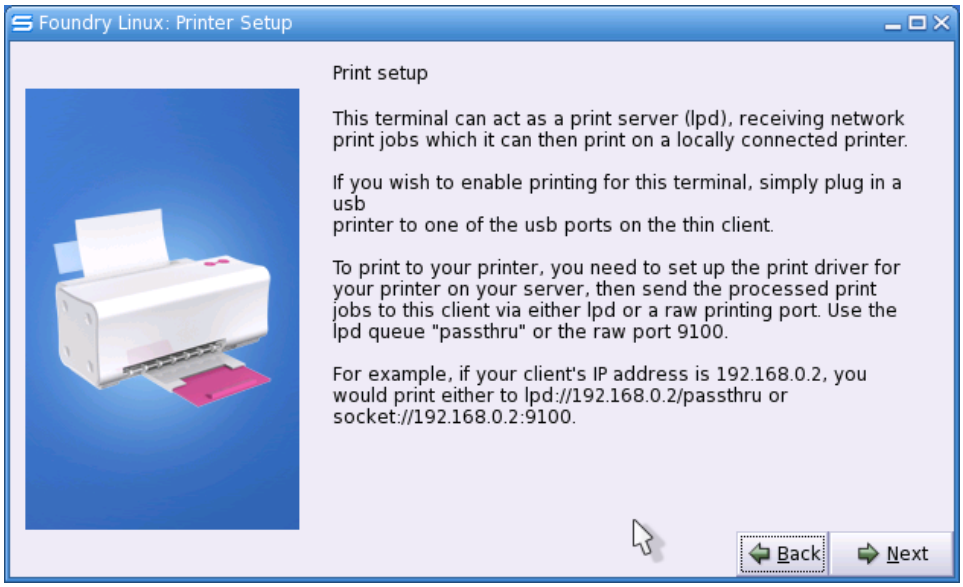

Foundry Linux: Printer Setup
Print setup
This terminal can act as a print server (lpd), receiving network print jobs which it can then print on a locally connected printer.
If you wish to enable printing for this terminal, simply plug in a usb
printer to one of the usb ports on the thin client.
To print to your printer, you need to set up the print driver for your printer on your server, then send the processed print jobs to this client via either lpd or a raw printing port. Use the lpd queue "passthru" or the raw port 9100.
For example, if your client's IP address is 192.168.0.2, you would print either to lpd://192.168.0.2/passthru or socket://192.168.0.2:9100.
Back
Next

Illustration 7: Setup Wizard - Print Setup Information Window

Copyright © 2008 William Matthew Limited. All rights reserved

The final window is a confirmation window informing you that the setup process is complete. Click “Finished” and the Setup Wizard will close, and the Connection Manager will be launched. You're now ready to configure your connections.

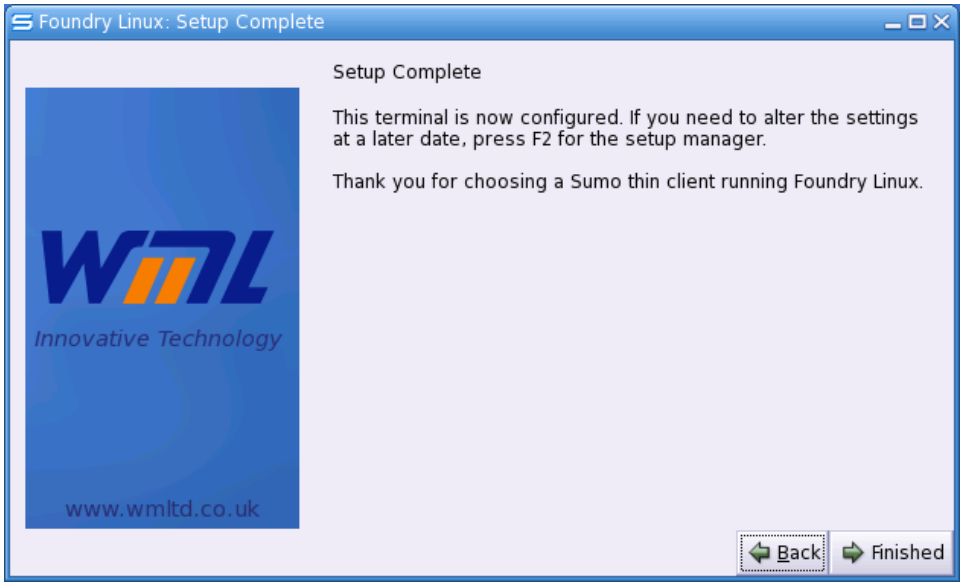

Foundry Linux: Setup Complete
Setup Complete
This terminal is now configured. If you need to alter the settings at a later date, press F2 for the setup manager.
Thank you for choosing a Sumo thin client running Foundry Linux.
Innovative Technology
www.wmltd.co.uk
Back
Finished

Illustration 8: Setup Wizard - Setup is Complete

Copyright © 2008 William Matthew Limited. All rights reserved

Client Connection Manager

The client connection manager runs every time the WML Linux Thin Client is powered up. It manages all of your connections and provides an interface for you to configure new connections. You can always return to the Connection Manager using the key combination Ctrl-Alt-End (except when initially running the Setup Wizard).

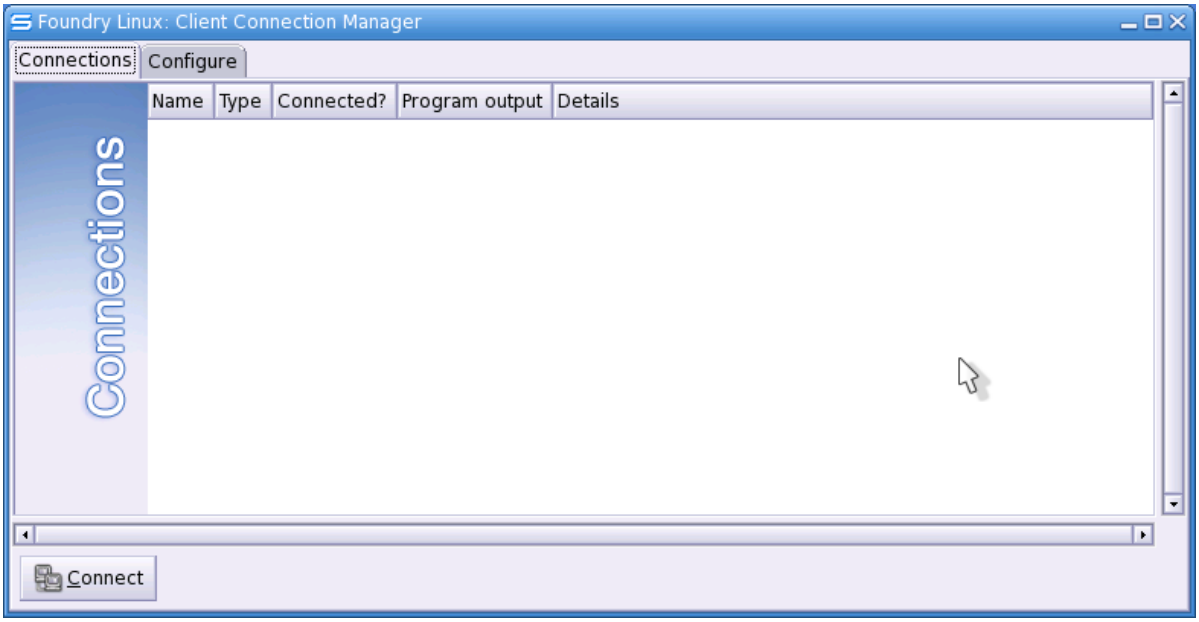


Illustration 9: A new, empty Connection Manager

The connection manager manages the windows of each running connection and allows you to switch between the windows using the key combination Ctrl-Alt-Down.

There are a variety of ways to connect to a local or remote server, WML recommend using **No Machine NX.** No Machine is a very cost effective and reliable method, it will allow multiple full graphic sessions to any machine that has the inexpensive No Machine server software loaded. With No Machine NX you can also run a low performance session to a remote server using a dial up modem, although this would be slow in terms of response times.

The connection manager also allows you to configure Citrix ICA, RDP, VNC, SSH, telnet, www and XDMCP connections. The setup of each connection is covered in the following sections.

Tooltips are provided throughout the Connection and Setup Managers, giving you context sensitive help.

Copyright © 2008 William Matthew Limited. All rights reserved

Connections Tab – Overview

The "Connections" tab of the Connection Manager is available to any user of the thin client. Illustration 10 shows a Connection Manager with two configured connections. One connection is called "Login to master server" and is of type xdmcp – it's an X windows connection. The second connection is a secure shell login called "Admin secure shell login". In this window, neither connection is currently highlighted.

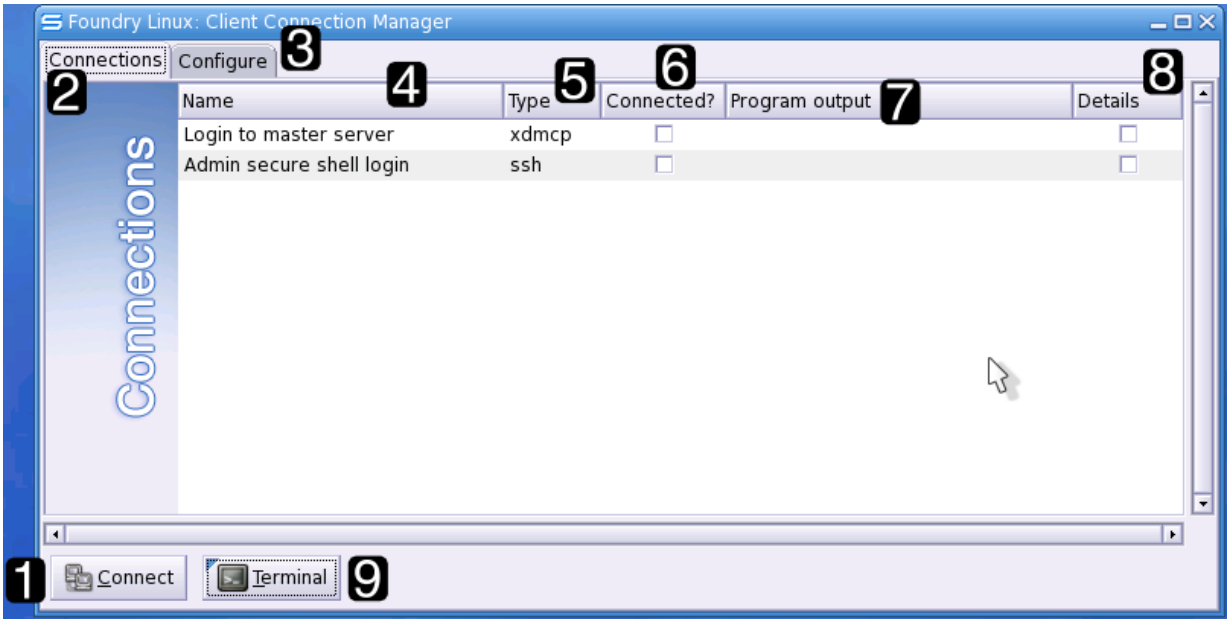


Illustration 10: An overview of the Connections tab of the Connection Manager

In Illustration 10, the numbered features of the interface are:

1. The Connect button. Launches the highlighted connection. If the highlighted connection is already connected, then the connection becomes the current connection.
2. The Connections tab is a lighter gray, showing that it is the selected tab.
3. The Configure tab is a darker shade of gray, showing that it is not selected.
4. The "Name" field shows the name of the connection, as given by the administrator.
5. The "Type" field shows the connection protocol.
6. The "Connected?" field will be checked for any connections which are currently active.
7. The "Program output" field shows the first line of any output generated by the connection, after it has finished. This can be useful for diagnosing failed connections due to network problems.
8. The "Details" field will be checked if the connection generates output. Click on the checkbox to view the full output in a separate screen.
9. The "Terminal" button is optional – it can be switched on in the Setup Manager. This is intended for power users and administrators. *Note that if the terminal is available, a user of the WML Linux Thin Client cannot be prevented from manually editing the connection configuration.*

Copyright © 2008 William Matthew Limited. All rights reserved

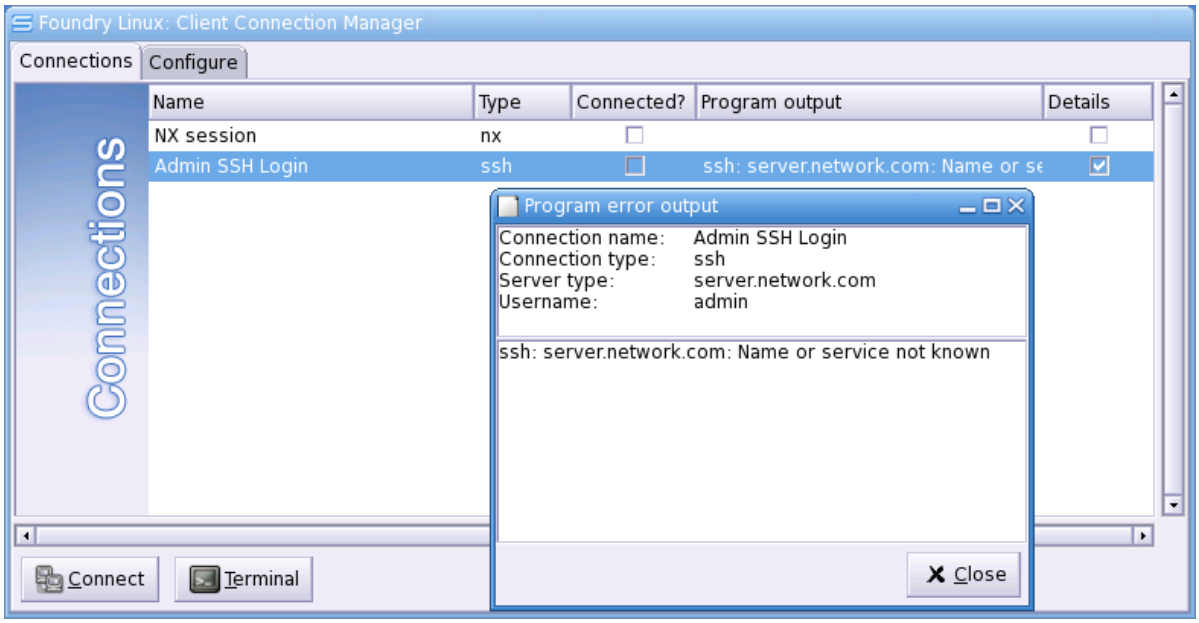


Illustration 11: The Program output window

In the example shown in Illustration 11, the output from ssh is that server.network.com is an unknown name, indicating that the domain name server couldn't resolve server.network.com into an IP address.

Copyright © 2008 William Matthew Limited. All rights reserved

Configuration Tab – Overview

The Configuration tab is password protected and is intended for the use of administrators. Illustration 12 shows the Configuration tab with the same connections configured as in Illustration 10

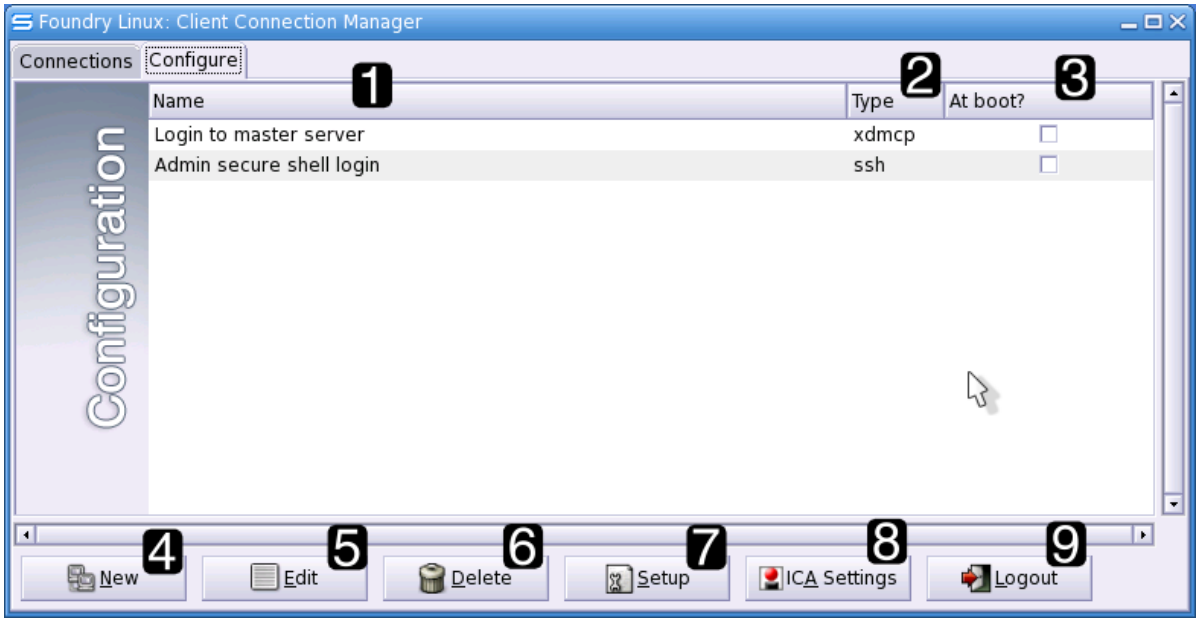


Illustration 12: An overview of the Configuration tab of the Connection Manager

The features of the Configuration tab are:

1. The "Name" field shows the name of the connection, as given by the administrator.
2. The "Type" field shows the connection protocol.
3. If the "At boot?" field is checked, the connection will be launched when the WML Linux Thin Client powers up. You can check and uncheck this field without opening the Connection Details window for the connection.
4. The "New" button is used to create a new connection.
5. The "Edit" button is used to edit an existing connection (highlight the connection then press "Edit").
6. The "Delete" button is used to delete a connection. Note that a running connection may not be deleted – first shut it down, then highlight its entry in the list and press the "Delete" button.
7. The "Setup" button launches the Setup Manager. This has the same effect as pressing the F2 key.
8. The "ICA Settings" button opens a window to configure certain settings which are used by the Citrix ICA client program for all ICA connections.
9. The "Logout" button ends your use of the Configuration tab. Once you have logged out, to add, edit or delete connections, you'll need to re-enter your password.

Copyright © 2008 William Matthew Limited. All rights reserved

Creating a new Connection

To set up any new connection, you need to switch to the "Configuration" tab of the Connection manager. You will be asked for the administration password, which is simply "password" for a factory delivered box.

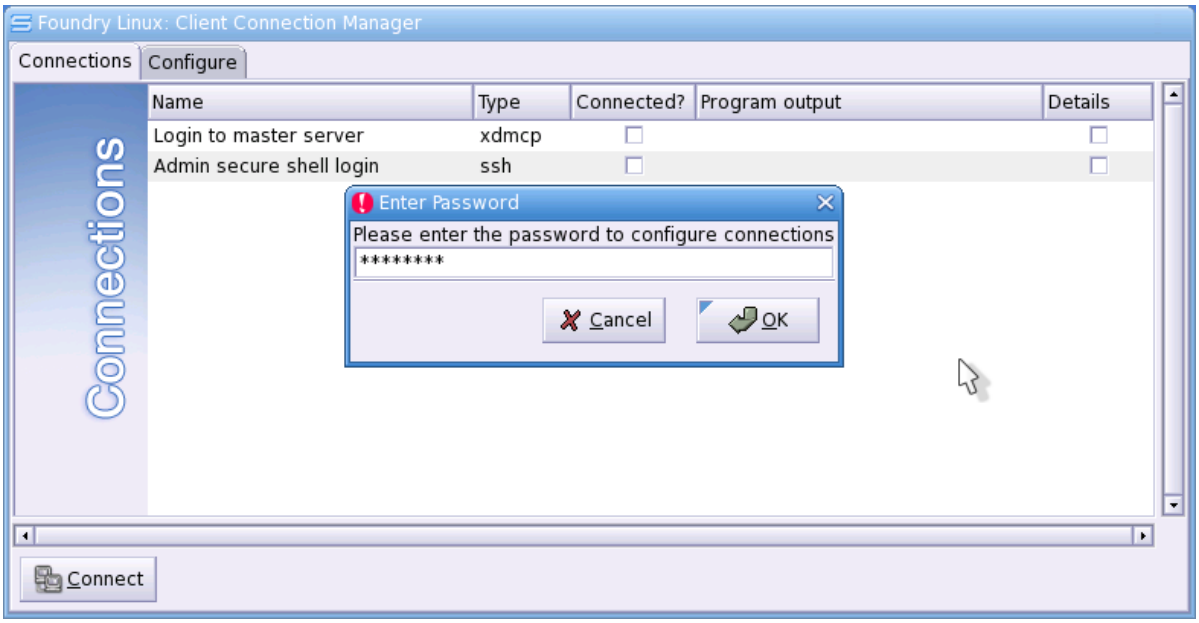


Illustration 13: Connection Manager - Entering the administration password

On the configuration tab, click on the "new" button to create a new connection.

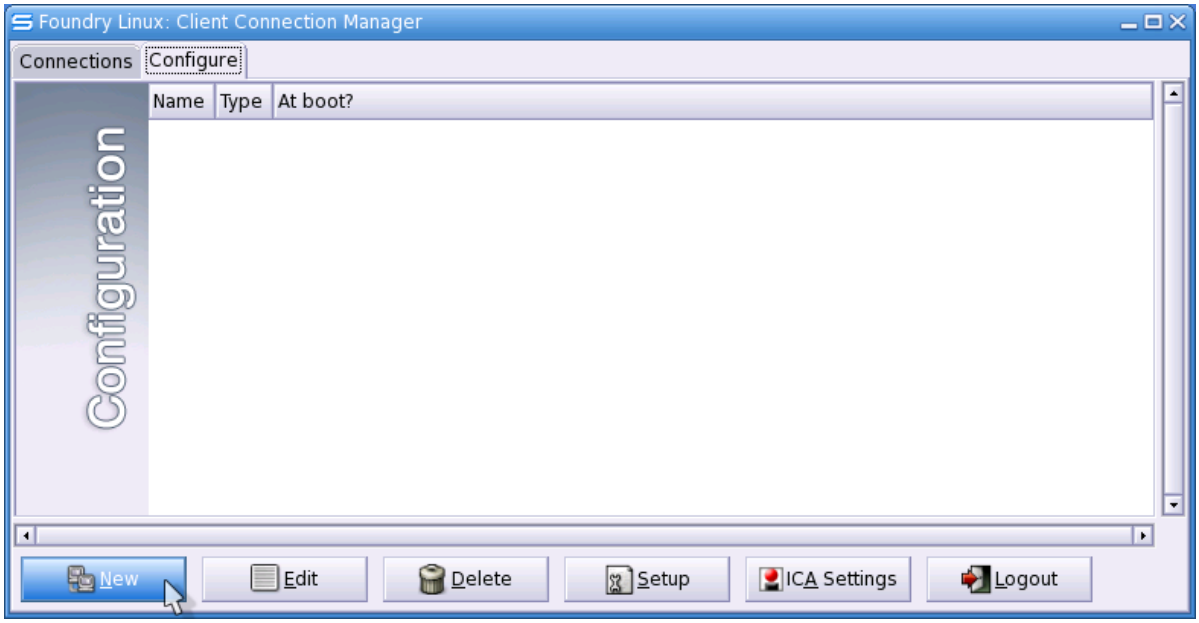


Illustration 14: Connection Manager – Clicking the "New" button to create a connection

Copyright © 2008 William Matthew Limited. All rights reserved

A window will appear with a drop-down menu from which you can choose the type of connection you want to create. In Illustration 15, a Nomachine NX connection is highlighted. Press OK, and the configuration window of the selected connection will appear, and you can then enter the details for the connection.

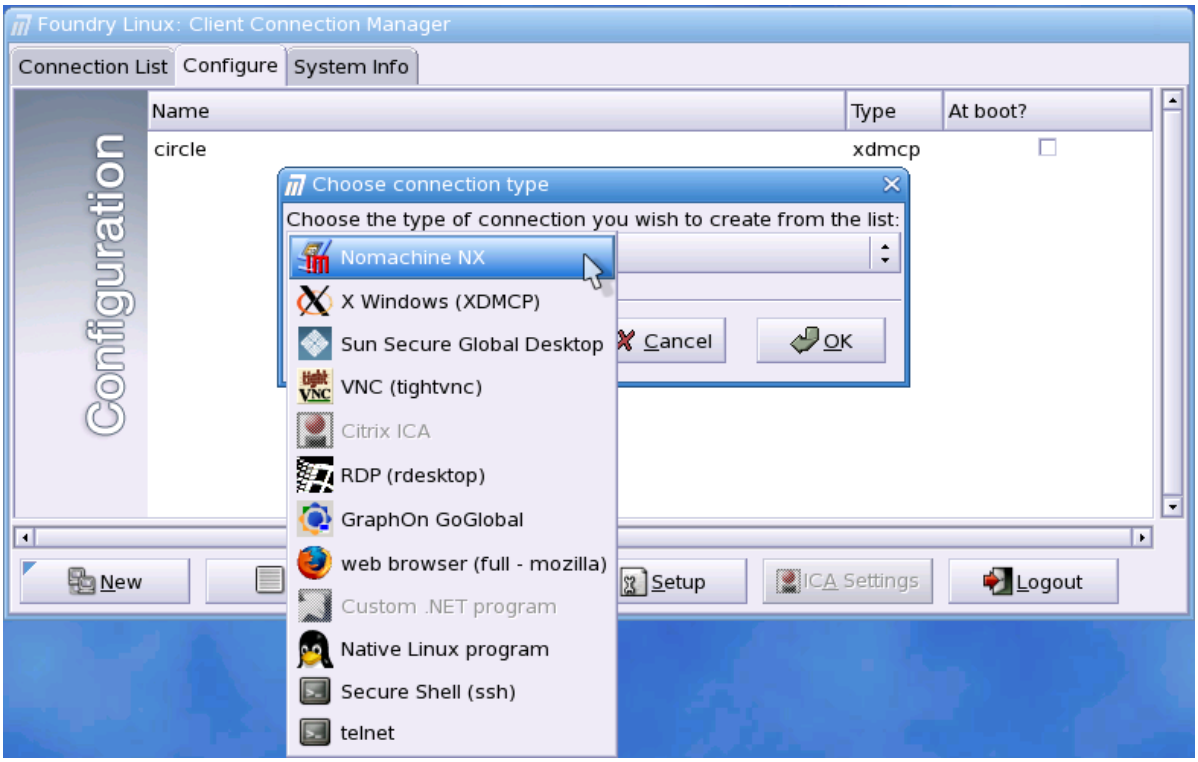


Illustration 15: Choosing a Nomachine NX connection

Copyright © 2008 William Matthew Limited. All rights reserved

Editing a Connection

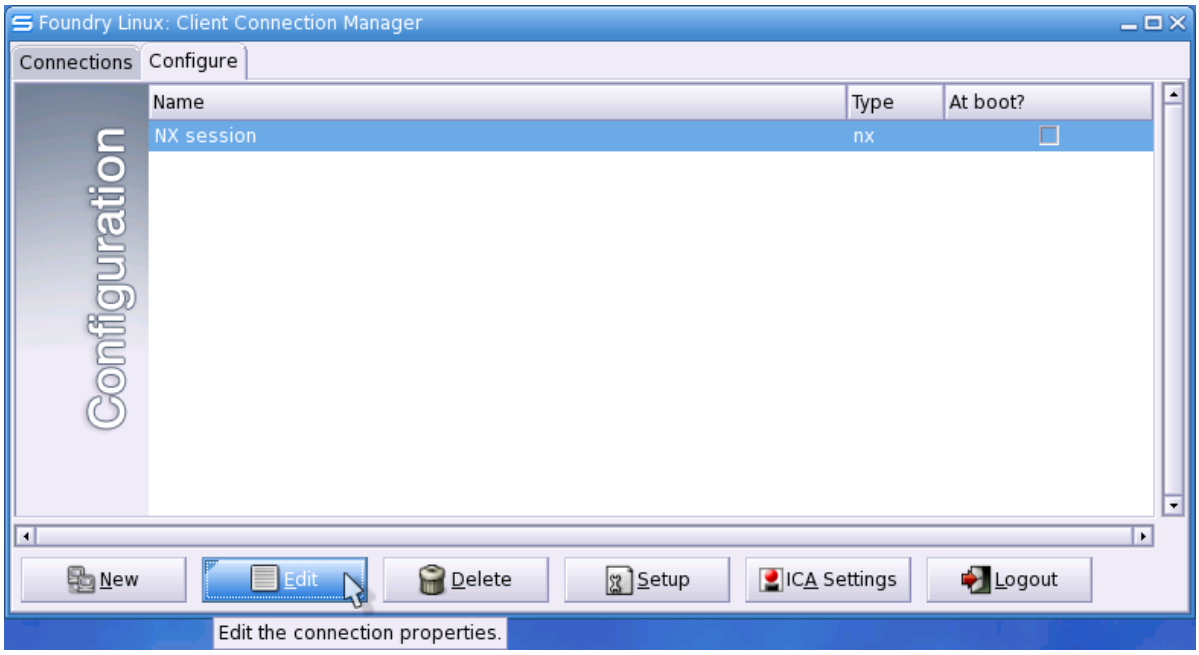


Illustration 16: Choosing "Edit" for the highlighted connection

To edit a previously configured connection, select the “Configuration” tab again, entering the password if necessary. Highlight the connection to edit, and press the “Edit” button. The relevant connection details window will appear and the configuration can be changed as normal.

NoMachine NX

If you are editing a Nomachine NX connection: If you previously elected to save the password of the user, the act of editing the connection will delete the stored password and the user will need to re-enter the password the next time the connection is run.

Citrix ICA

Once you have created an ICA connection with a given connection name, you can no longer change that name when you edit the details of the connection. All other details of the connection may be changed.

Copyright © 2008 William Matthew Limited. All rights reserved

NoMachine NX

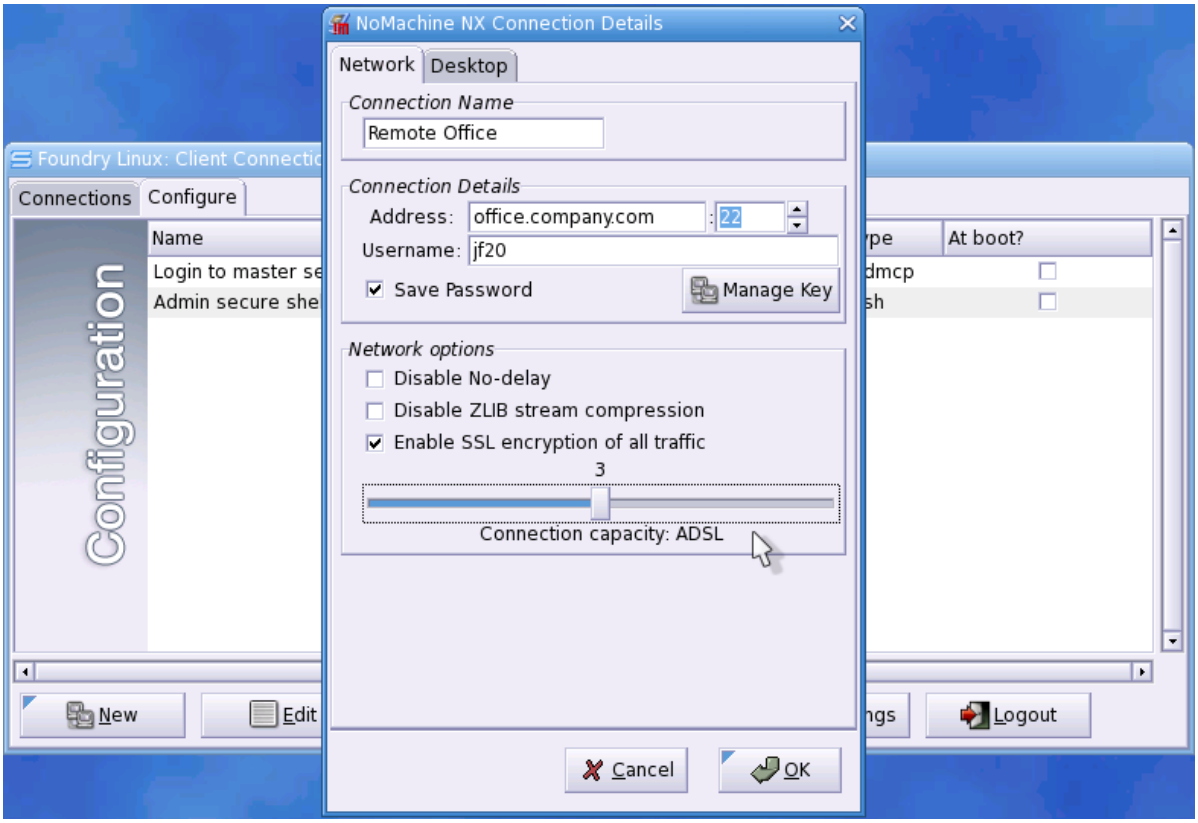


Illustration 17: Entering network details for Nomachine NX connection

Create a new connection of type Nomachine NX. The NoMachine NX Connection Details window will appear with the "Network" Tab pre-selected. This window provides an interface to create the NX session . When the session is launched, NoMachine's own NX Client program is used to launch the connection.

NoMachine NX: Network Tab

The NoMachine NX Connection Details window has fields for the connection name and the network details – server address, port, username etc. You can also select a number of options to control how the NX connection behaves.

In Connection Name, enter the name of the connection, as you want it to appear in the Connection Manager. The Connection Name may include spaces, but none of the characters: `" ' = , . ; : / \`.

In the address field, enter either the network name or the IP number of the NX server. The port to connect to is usually the same as the SSH port (22) but this is not always the case. Enter the username for the connection and check the checkbox if the password should be stored on the thin client between reboots. If stored, it will be kept in hashed form in the connection's .nxs file.

Copyright © 2008 William Matthew Limited. All rights reserved

Optional: NX key

NX connections use SSH to encrypt the connection between the client and server and as such NX is the most secure graphical thin client connection available. The login process uses a two-stage process. The first login uses a key-based login. A standard NX key is supplied as a default, and using this key, a client can proceed to the second secure login, which uses a password as authentication token. If you use the default NX key on your server, then any client can pass the stage 1 login, and can attempt to use password based login to gain access to the server. This remains secure, but relies on quality passwords.

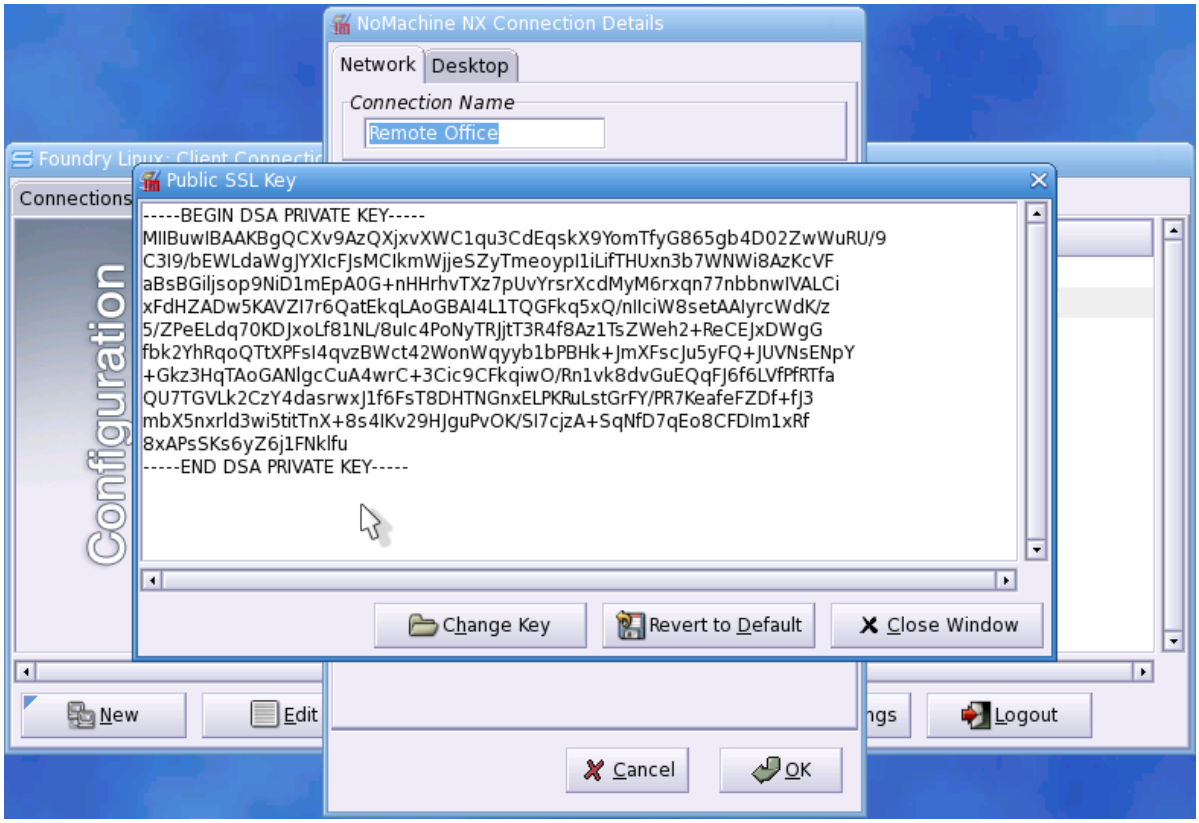


Illustration 18: Managing the NX SSL key

To increase the security of your connection, you can replace the default key on your NX server. Please refer to Nomachine's documentation on setting up the NX server. Once you have generated a non-standard key for the stage 1 login, you need to load it onto your WML Linux Thin Client. Put the key file on a USB pen-drive and plug it into your WML Linux Thin Client. Press the “Manage Key” button in the NX Connection Details window. The Public SSL Key window will appear. While you could technically type in the key, it would be a thankless task. Press the “Change Key” button to open a file dialog, which will allow you to find the key on your USB drive.

Copyright © 2008 William Matthew Limited. All rights reserved

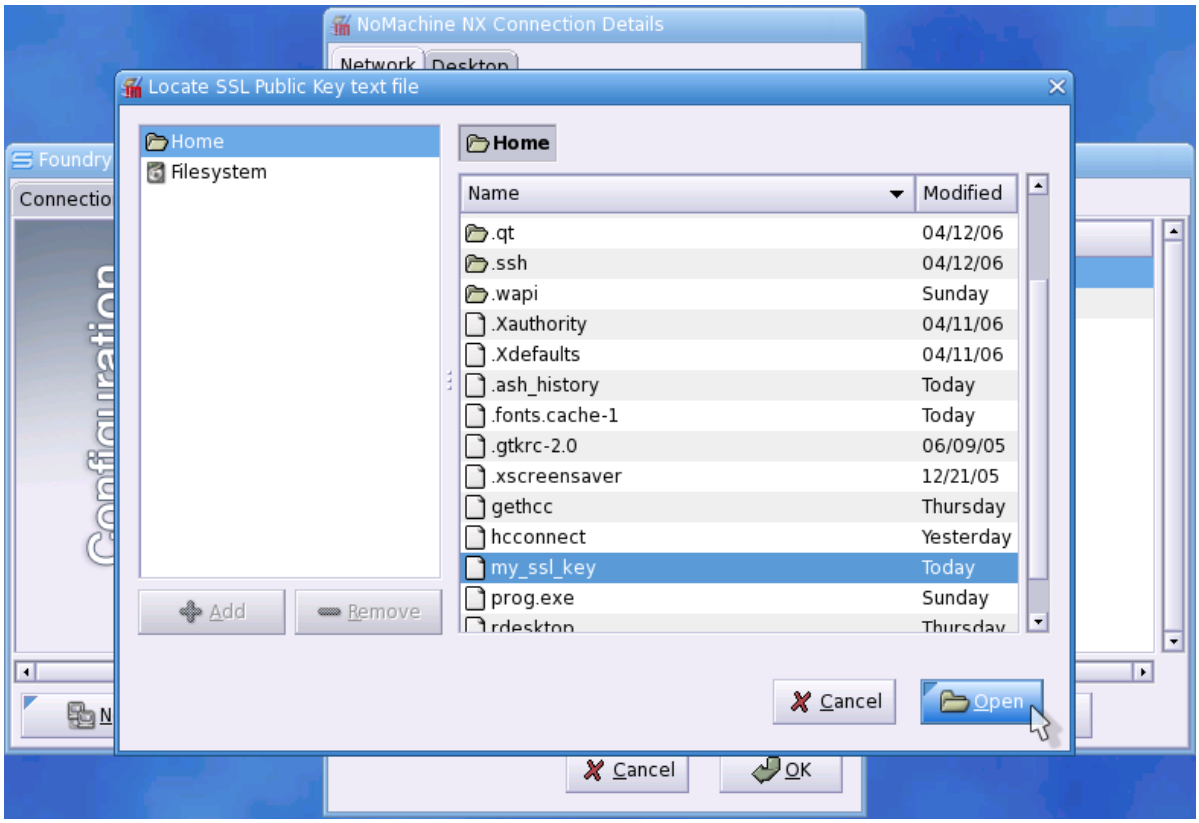


Illustration 19: Browsing for an SSL key

The illustration shows a user choosing "my_ssl_key" which is in the "Home" directory – this user possibly transferred the file to the thin client using a web browser or the sftp client. To access your key on a flash drive, you will need to click on the "Filesystem" icon, then choose the "flash" directory. Click "Open" and the contents of the file will appear in the Public SSL Key window. Close the Public SSL Key window and proceed with setting up the NX connection.

NoMachine NX: Desktop Tab

The "Desktop" Tab (Illustration 20) allows you to choose the type of desktop to launch using the NX Client. The main choices given are GNOME, KDE, CDE. Most users will choose GNOME or KDE. To find out more about launching custom sessions and applications, please refer to the Nomachine documentation – this setup window has the same options as Nomachine's own NX client. Refer to Nomachine also for more information about setting the XDM Settings.

The Window Size option allows you to choose whether your NX session will appear in a managed window on the WML Linux Thin Client desktop, or as a fullscreen window occupying the entire display.

Images are encoded by the NX compression protocol using JPEG, PNG or Xbitmap formats. The image encoding drop-down menu allows you to specify which should be used, or "Default" will allow NX to choose based on the speed of the connection, as specified on the Network tab. JPEG offers the best compression for low bandwidth connections, but as it is a lossy compression format, the image quality of your screen will not be as good compared with PNG or Xbitmap formats. With JPEG image encoding, the quality may be chosen. Set the quality to low for the slowest connections.

Copyright © 2008 William Matthew Limited. All rights reserved

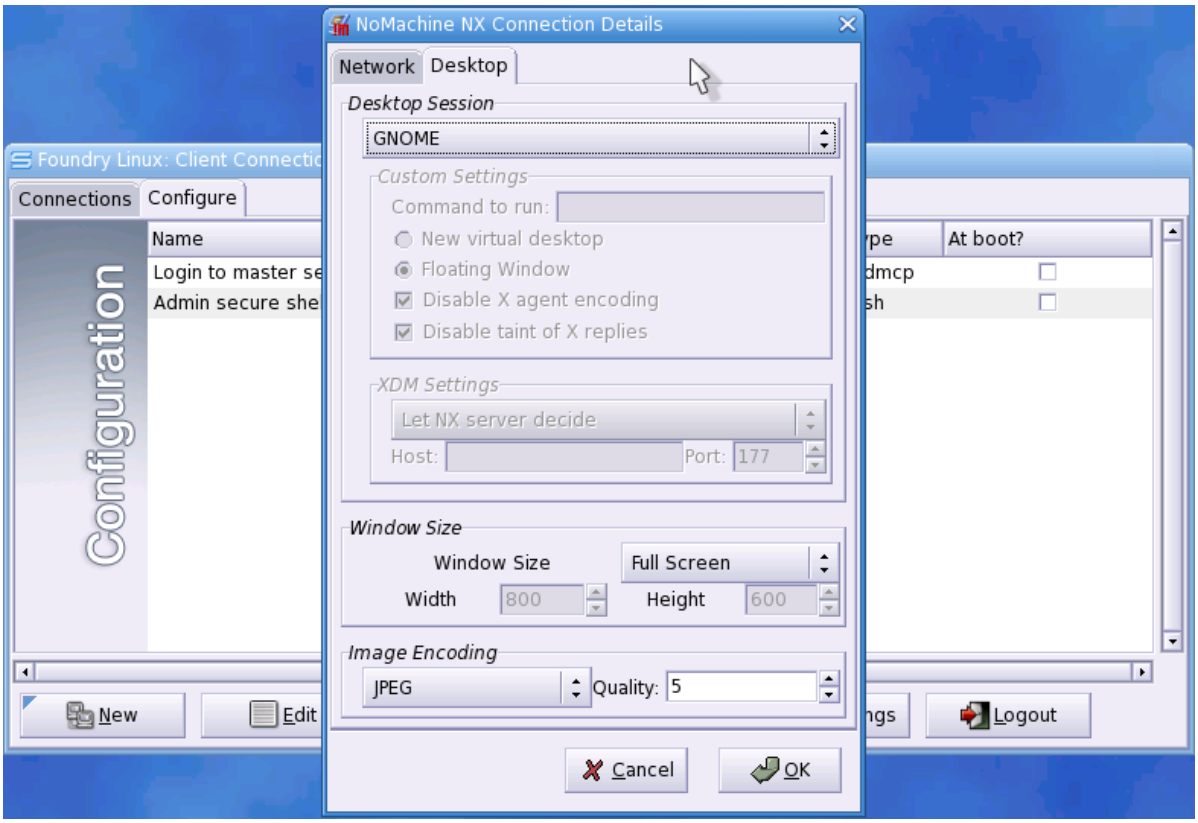


Illustration 20: The "Desktop" tab of the Nomachine connection details window

When you have entered the settings correctly, press “OK” and your connection will appear in the list of connections in the Connection Manager.

Launching an NX Connection

Switch back to the Connections Tab on the Connection Manager, highlight your new NX connection, then click the “Connect” button to launch it.

Copyright © 2008 William Matthew Limited. All rights reserved

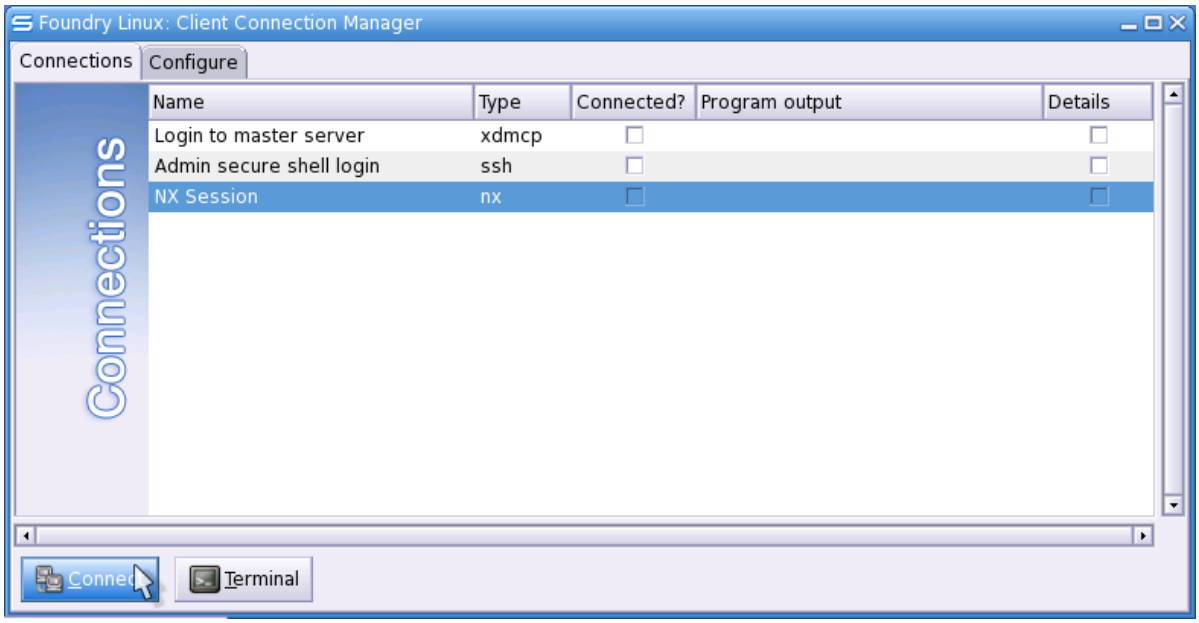


Illustration 21: Launching the new NX session

The Nomachine NX client Login window appears and the user can enter his username. The username may also be changed at launch time. The username field will always be filled in with the last username used to connect to the server

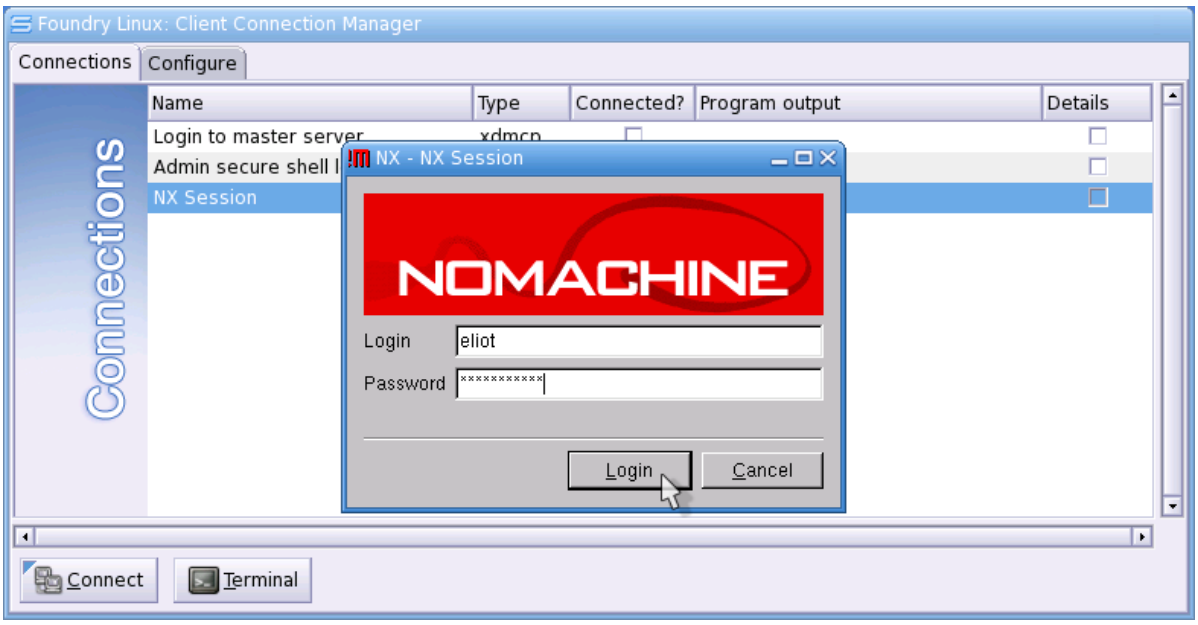


Illustration 22: The Nomachine NX Login details window

Once "Login" has been clicked, the NX client will connect to the server, authenticate the user and launch the desktop session.

Copyright © 2008 William Matthew Limited. All rights reserved

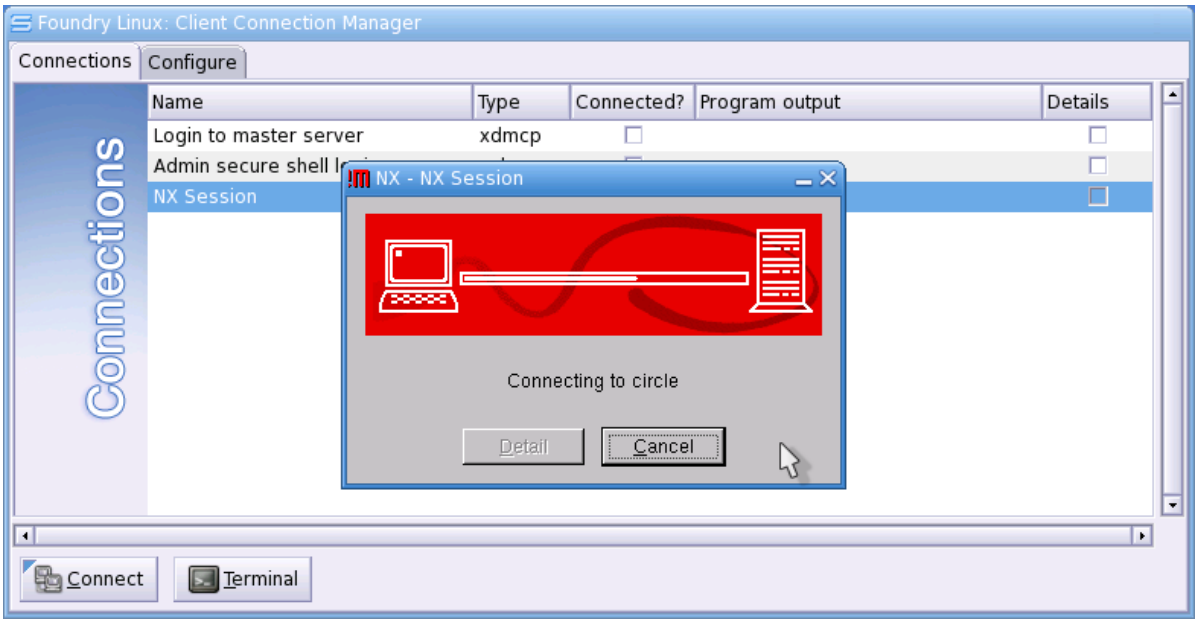


Illustration 23: During authentication, the NX client will display progress information

The desktop then appears, if authentication is successful. A message about the NX cachewill be displayed the first time the user logs onto the server. This message is a normal part of the NX connection procedure. It will not be displayed if the user logs off the server, then logs on again, as long as the thin client hasn't been rebooted. If the thin client is rebooted, and the user logs on to the server, the NX cache message will be shown again. This is because the NX cache files are stored in a volatile RAM disk on the WML Linux Thin Client.

Copyright © 2008 William Matthew Limited. All rights reserved

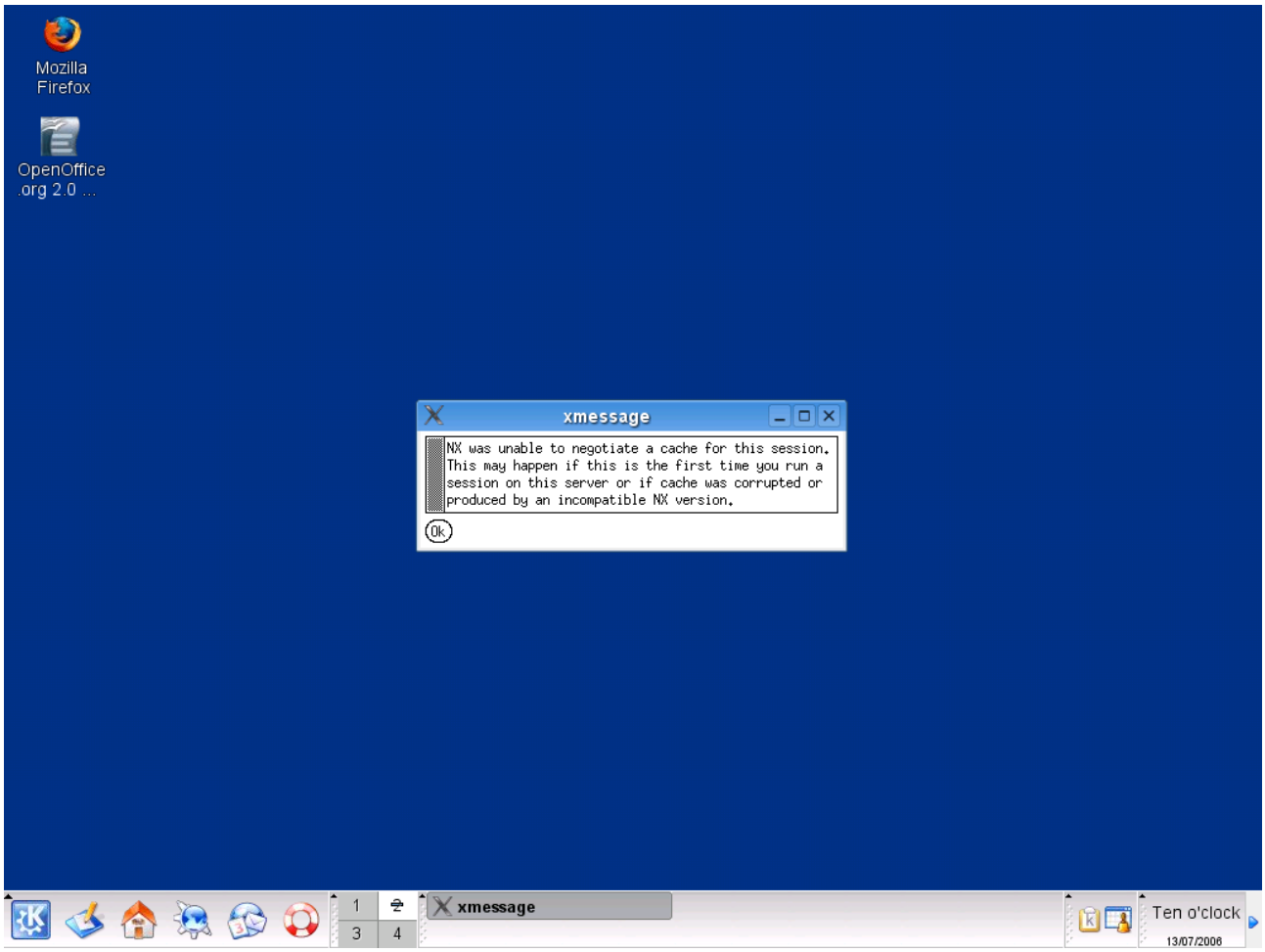

Mozilla Firefox
OpenOffice .org 2.0 ...
xmessage
NX was unable to negotiate a cache for this session. This may happen if this is the first time you run a session on this server or if cache was corrupted or produced by an incompatible NX version.
Ok
1
3
4
xmessage
Ten o'clock
13/07/2006

Illustration 24: The common NX cache information message

Press “OK” to acknowledge the cache message and proceed with your work as normal!

Copyright © 2008 William Matthew Limited. All rights reserved

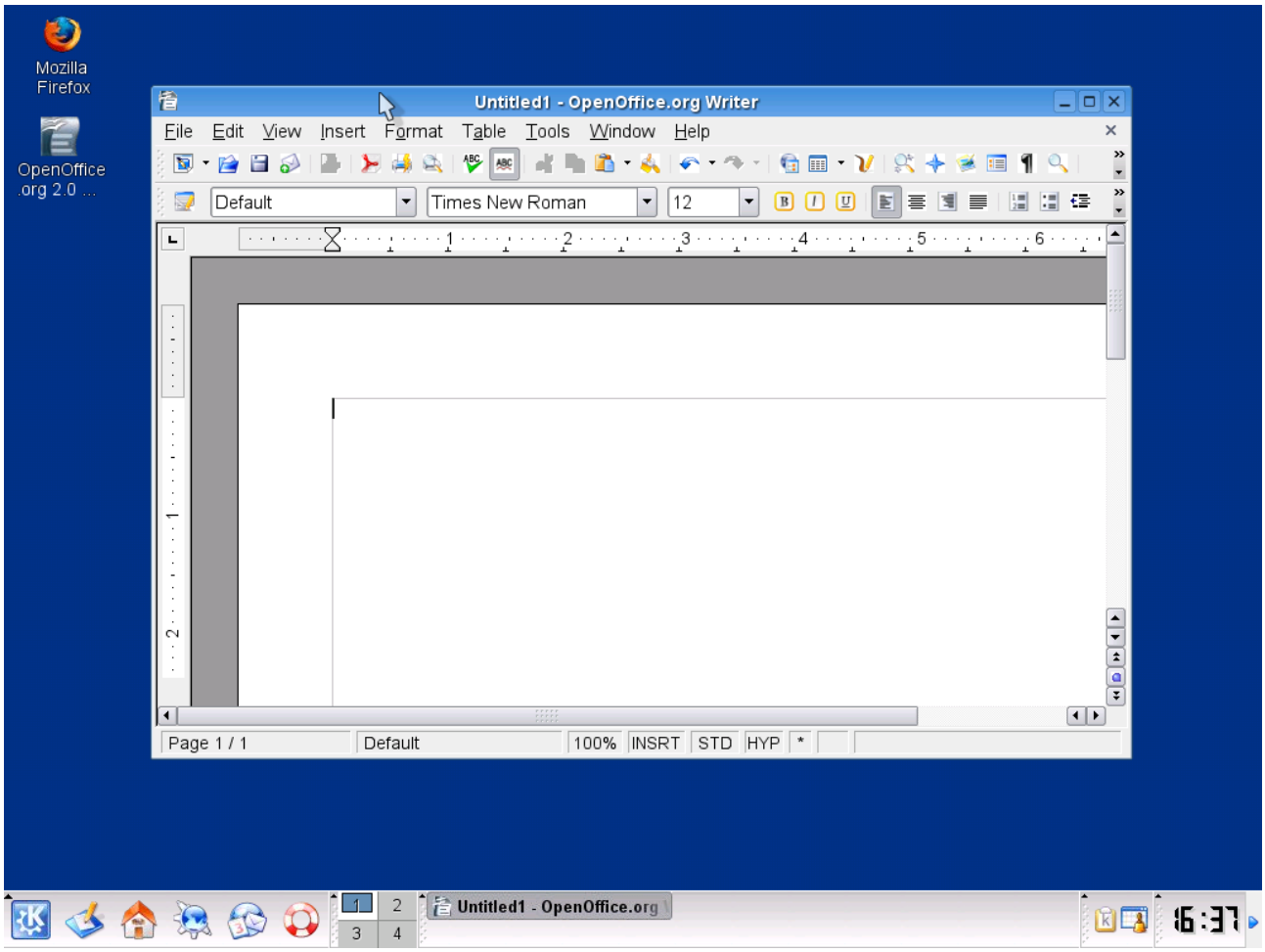


Illustration 25: A new KDE desktop session with OpenOffice.org word processor, delivered via Nomachine NX

Editing an existing NX connection

Editing a connection is very similar to creating anew connection, except that you select apre-existing NX connection in the “Configure” Tab of the Connection Manager, and then click the “Edit” button. The Nomachine NX Connection Details window will appear, with the existing settings. Simply edit the details as necessary, and click “OK”.

Copyright © 2008 William Matthew Limited. All rights reserved

Citrix ICA

In the Configuration tab, click "New" and select "Citrix ICA" from the drop down menu. The Citrix ICA configuration window will appear. The tabbed window follows the format of Citrix's own Linux client program. Please refer to their documentation for connections details.

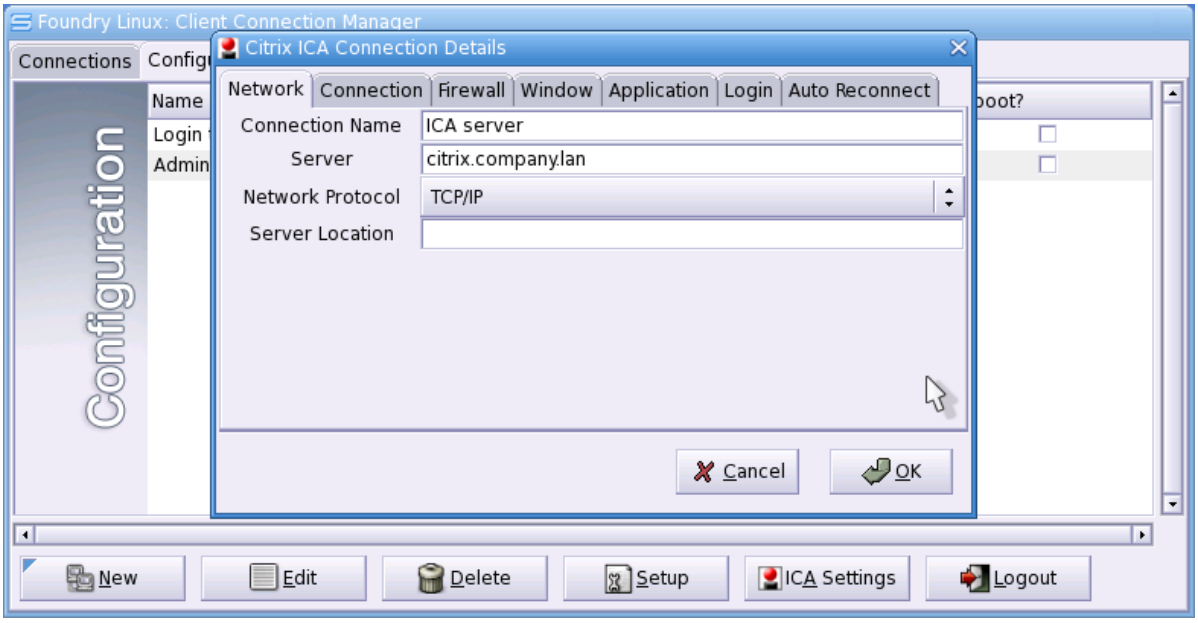


Illustration 26: Citrix ICA Connection Details window

The simplest ICA connection can be set up simply by filling in the "Connection Name" and "Server" fields and setting the Network Protocol to "TCP/IP". Unlike the other connection types, the connection name cannot subsequently be changed after the "OK" button has been clicked and the ICA connection created.

The "Window" tab allows the window size to be configured – as with all the supported connections, it defaults to being fullscreen.

Sound support

If you wish to use sound in your ICA connection, make sure you switch off the esound daemon in the Setup Manager. In the "Connection" tab you can then check the "Enable sound" checkbox and choose the sound quality setting.

Local USB storage device access

You can access a local USB drive within your Citrix session. To do so, you need to click the "ICA Settings" button in the Configuration tab of the Connection Manager and choose the "Drive Mapping" tab of the "Citrix ICA Settings" Window. Click the "enable drive mapping" checkbox and enter the drive letter you would like the drive to appear as on your Citrix desktop. This is shown in Illustration 27.

Copyright © 2008 William Matthew Limited. All rights reserved

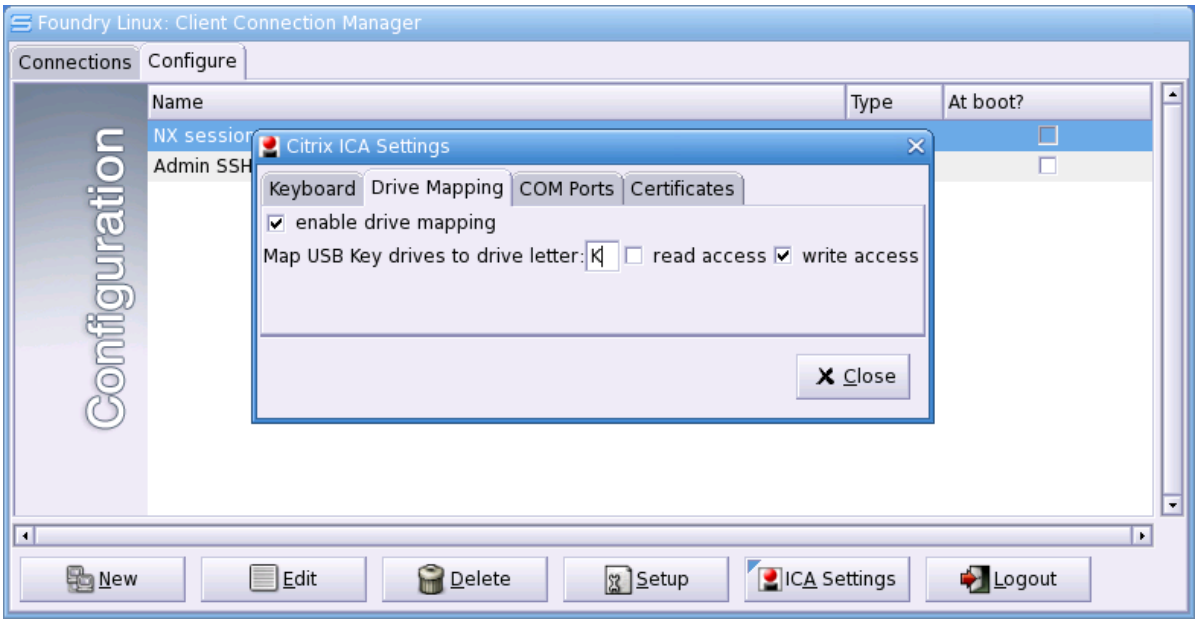


Illustration 27: Enabling drive mapping in Citrix ICA Settings

Copyright © 2008 William Matthew Limited. All rights reserved

RDP: Remote Desktop Protocol

RDP allows you to connection the WML Linux Thin Client to a Microsoft Terminal Server. It also allows you to connect to a Microsoft Windows XP Pro desktop PC. RDP Connections are very easy to configure.

To create a new RDP connection, click "New" in the Configuration tab and select "RDP (rdesktop)" from the drop down menu. The "RDP Connection Details" window will appear.

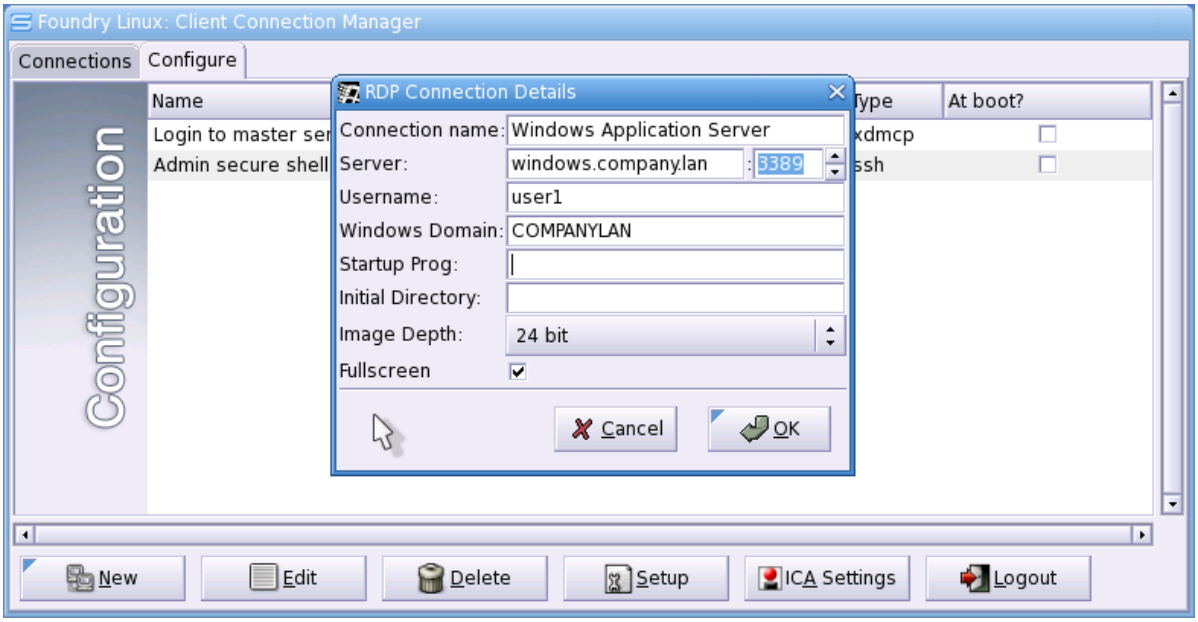


Illustration 28: Editing connection details for a new RDP connection

Fill in the Connection name with the text which will identify the connection in the Connection Manager.

In the "Server" field, enter the IP address or the network name of the Terminal Server.

Note that you cannot simply enter the Windows name of the computer unless this is the same as the tcp/ip network name.

The port defaults to 3389, which is the standard port number used by the RDP protocol. Change this only if you know it is different for your server.

The "Username" and "Windows Domain" fields are optional, and can be changed when the connection is run.

The "Startup Prog" and "Initial Directory" fields are optional and can be used to run scripts when the user logs in.

The "Image Depth" field controls how many colours to use for the connection. If 24 bit is chosen, but the server only supports 8 or 16 bit colour, then the RDP client will fall back to the highest supported resolution.

Uncheck the "Fullscreen" checkbox to run the RDP connection in a managed window.

rdesktop is always called with the options -r sound:local and -r disk:usbdisk=/flash to allow sound output in RDP sessions and usb flash disk access. Note that you must stop esound from running if you wish to use sound in RDP connections.

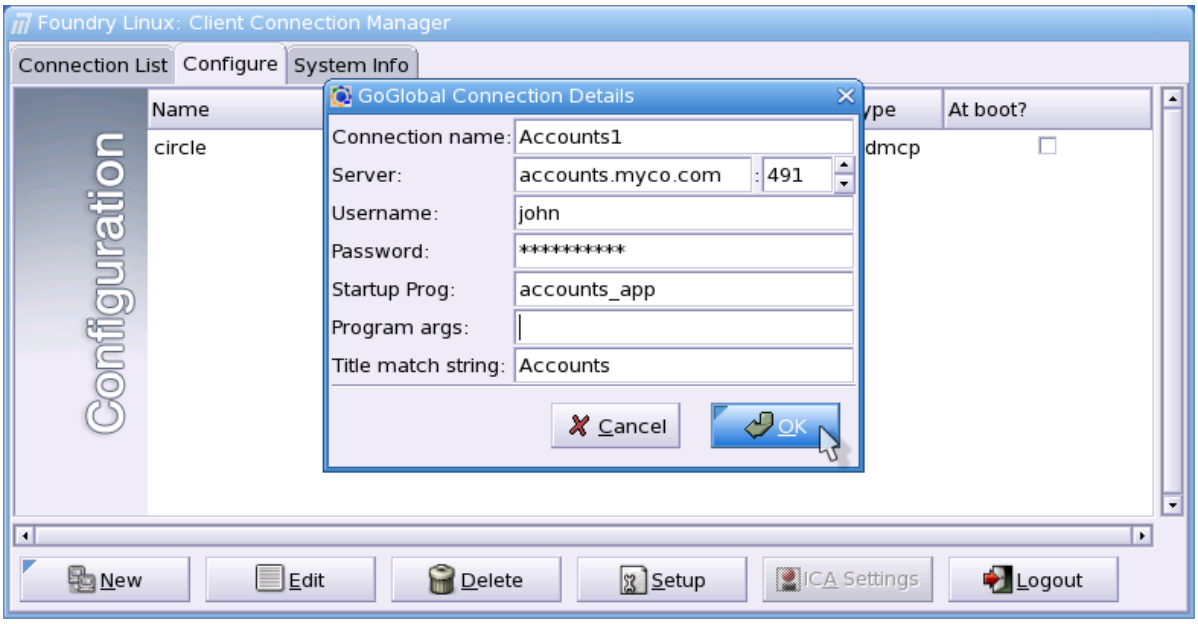
Copyright © 2008 William Matthew Limited. All rights reserved

GraphOn GoGlobal For Windows

The GraphOn GoGlobal protocol allows you to deliver Windows applications onto the WML Linux Thin Client Desktop, but differs from RDP in some important respects. It is based on its own proprietary protocol (RXP) and not Microsoft's RDP protocol. This means that Microsoft Terminal Services licences are *not necessary* to run GraphOn GoGlobal connections. GraphOn GoGlobal delivers a Program Launcher window, which can be used to deliver individually published Windows applications, without the entire Windows desktop being present.

To create a new GoGlobal connection, click "New" in the Configuration tab and select "GraphOn GoGlobal" from the drop down menu. The "GoGlobal Connection Details" window will appear.

Illustration 29: Editing connection details for a new GoGlobal connection



Fill in the Connection name with the text which will identify the connection in the Connection Manager.

In the "Server" field, enter the IP address or the network name of the GoGlobal Server.

Note that you cannot simply enter the Windows name of the computer unless this is the same as the tcp/ip network name.

The port defaults to 491, which is the standard port number used by GraphOn's RXP protocol. Change this only if you know it is different for your server.

The "Username" and "Password" fields are optional, and can be entered when the connection is run. If both are specified here, they must be valid (the user won't be given the option to change them).

The "Startup Prog" and "Program Arguments" fields are optional. Set the "Startup Prog" to exactly match the name given in the GoGlobal Cluster Manager "Name" field in the "Applications" tab. This will run the GoGlobal client so that it will omit the "Program Window" and launch straight into the application. "Program Arguments" are passed to the launched program.

Note that there is unfortunately a limitation when running individual applications in this way. If two applications are published, you cannot create two Foundry connections to individually launch each

Copyright © 2008 William Matthew Limited. All rights reserved

application. In this case, leave the "Startup Prog" field blank to have the GoGlobal program manager launched.

The "Title match string" field should only be filled in when creating connections which will launch individual applications rather than the GoGlobal Program Window. It is used to help the Foundry Linux Connection Manager manage the running connections. Enter a string which will identify the window of the program which will launch. For example; if the program to be launched is Internet Explorer, the string "Windows Internet Explorer" will always appear in the title bar. Enter "Windows Internet Explorer" into the "Title match string" field.

Copyright © 2008 William Matthew Limited. All rights reserved

X Windows - XDMCP

X Windows is used by almost every Unix and Linux machine with a graphical desktop. You can connect to *any* Linux PC or server using XDMCP – the X Display Manager Control Protocol. However, most Linux distributions ship with this feature switched off for the sake of security. To enable it refer to your distribution's documentation. *Hint: The file /etc/X11/xdm/Xaccess should be configured to allow XDMCP connections, and your Login manager must also be configured to allow remote connections; see gdmsetup for the GNOME display manager, /etc/X11/xdm/xdm-config for the X Display Manager and kdmctl for the KDE display manager.*

To set up an X Windows connection, follow the usual procedure, choosing "X Windows (XDMCP)" in the drop down menu of the "Choose connection type" window.

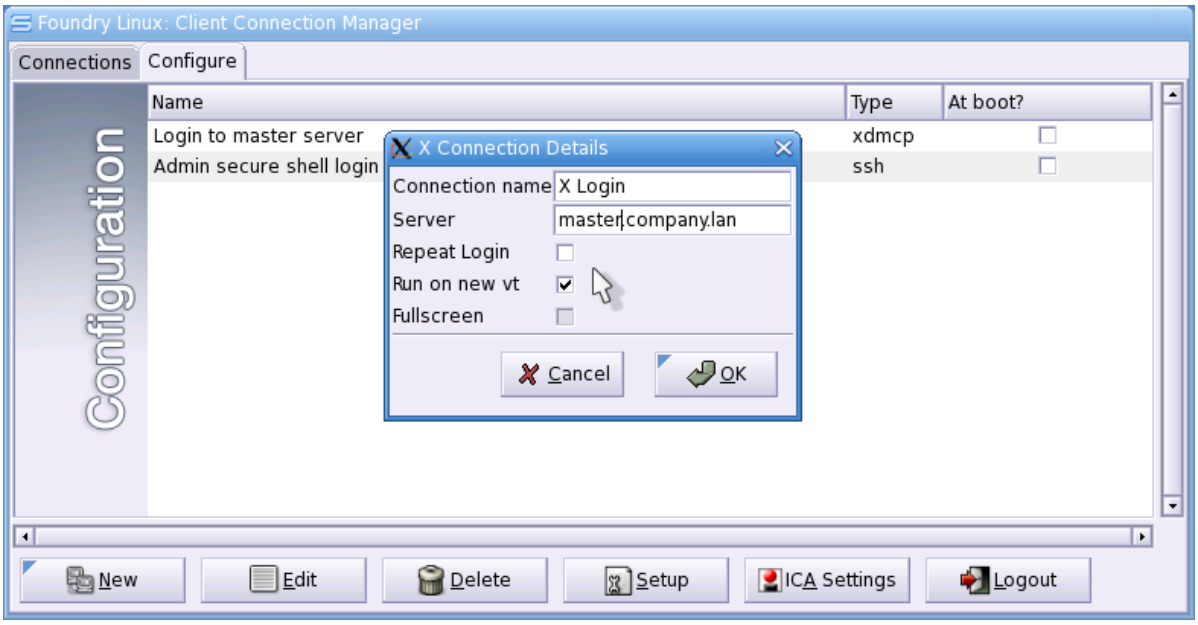


Illustration 30: Filling in the details for an X Windows connection

As with all the other connections, the "Connection name" identifies the connection and the server is the computer to connect to, either by TCP/IP network name or IP address.

Check "Repeat Login" if you want the Login window for your Linux/Unix server to reappear after a user logs out.

"Run on new vt" is checked by default and means that the X connection will run on a new virtual terminal in genuine fullscreen mode. If this is unchecked, then the X connection will run in a managed window. If you then check "Fullscreen", the managed window will occupy all of the display area. Note that running in a managed window is slower than running your X connection on a new vt.

XDMCP Broadcast

If you want to connect to any willing XDMCP broadcast server on your network, enter "broadcast" in the "Server" field instead of a server network name or IP address.

Copyright © 2008 William Matthew Limited. All rights reserved

X Font Servers

By default, the WML Linux Thin Client uses a limited number of fonts provided by its own X font server. For information about configuring your WML Linux Thin Client to use fonts from another X font server on your network, see the Setup Manager sections.

Copyright © 2008 William Matthew Limited. All rights reserved

VNC – TightVNC

VNC is a well established protocol for providing access to a graphical computer session via a network. VNC servers are available for Unix/Linux and Windows computers.

The WML Linux Thin Client ships with the TightVNC vnc viewer program, which extends the VNC protocol adding extra compression to the connection, by using JPEG image compression – the original VNC protocol sent uncompressed bitmap images over the network.

Open a new connection and choose "VNC (tightvnc)" from the drop down menu.

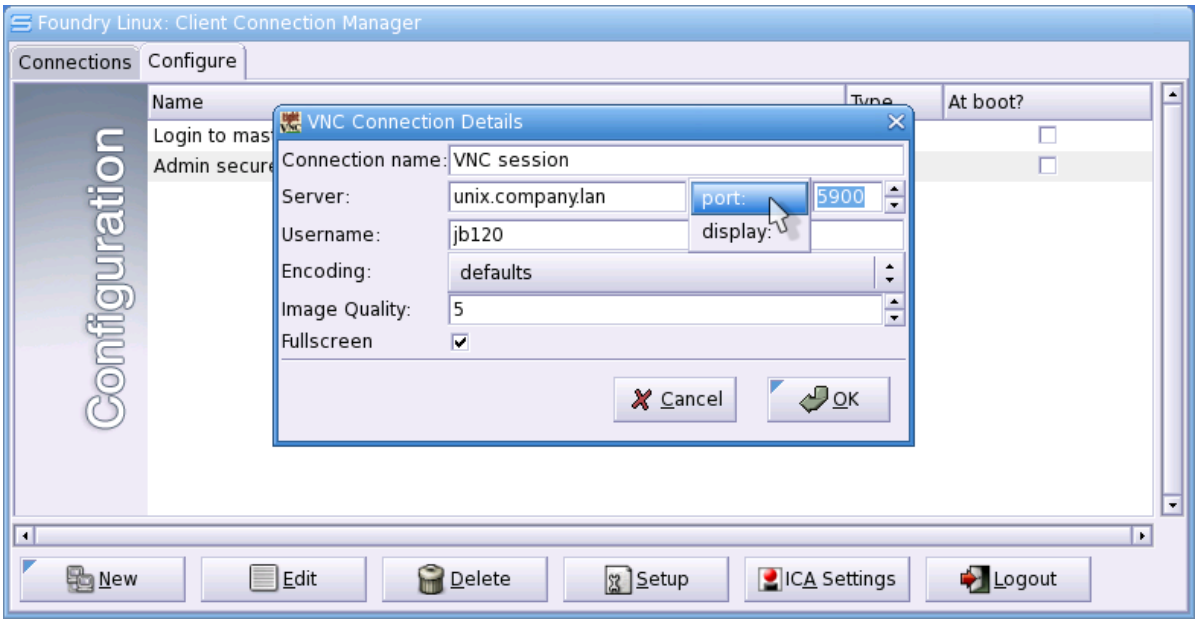


Illustration 31: Configuring a VNC connection

"Connection name" and "Server" are used to identify the connection and control which server to connect to. Like RDP, SSH, telnet and NX connections, the port can be configured, but with VNC, an alternative to specifying the port is to specify the display number. Illustration 31 shows a user changing from port to display.

The "Username" field is optional, some VNC servers will not require a username.

The "Encoding" field refers to image encoding. If this menu is left as "defaults" a range of image encodings will be tried. To specify a particular encoding, select from the list. Possible encodings are: copyrect, tight, hextile, zlib, corre, rre and raw. "tight" encoding uses JPEG compression and is the recommended setting. This is the first encoding to be tried if "defaults" is selected.

"Image quality" is used to specify the amount of JPEG compression used if "tight" encoding is chosen.

The "Fullscreen" checkbox determines whether the session will run fullscreen or in a managed window.

Copyright © 2008 William Matthew Limited. All rights reserved

Secure Shell - SSH

Secure shell (openssh) connections use shared key encryption to protect the data transmited between client and server. This is a very secure form of text-mode terminal connection. The SSH Connection Details window is simple, with just four fields.

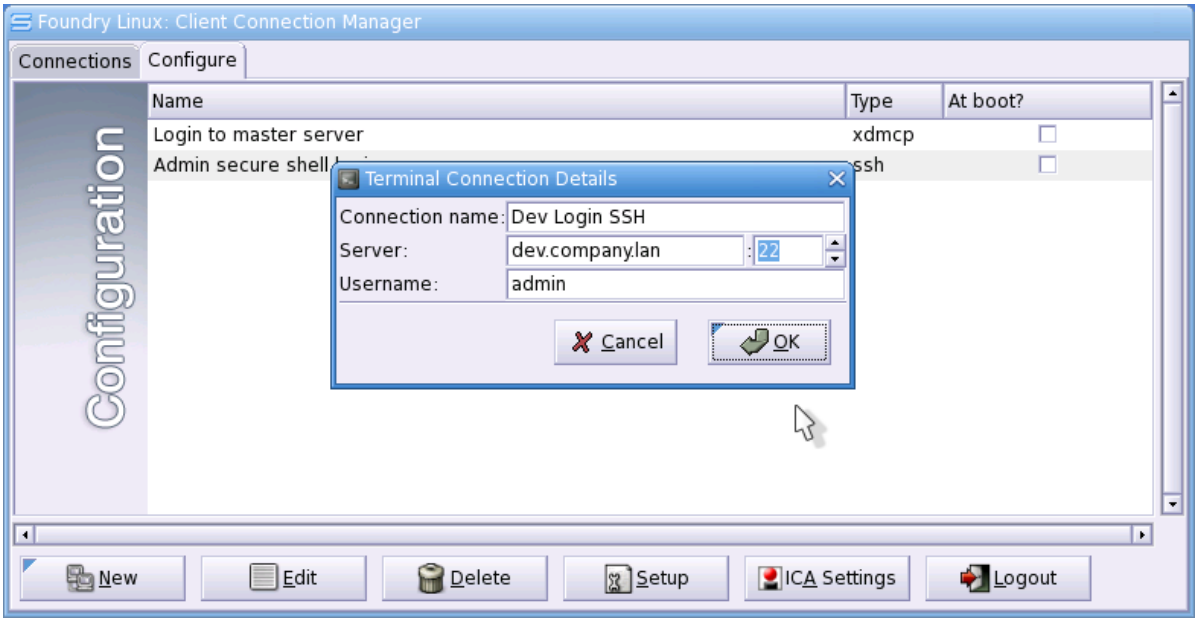


Illustration 32: Adding a secure shell connection

The Connection name and Server fields are common to all connections. As with other connections, the "Server" field should be filled in with the DNS network name or IP address of the ssh server. The port defaults to 22, the usual port on which ssh server daemons run. The "Username" field is optional. If left blank, the user will be asked for a username when the connection is started.

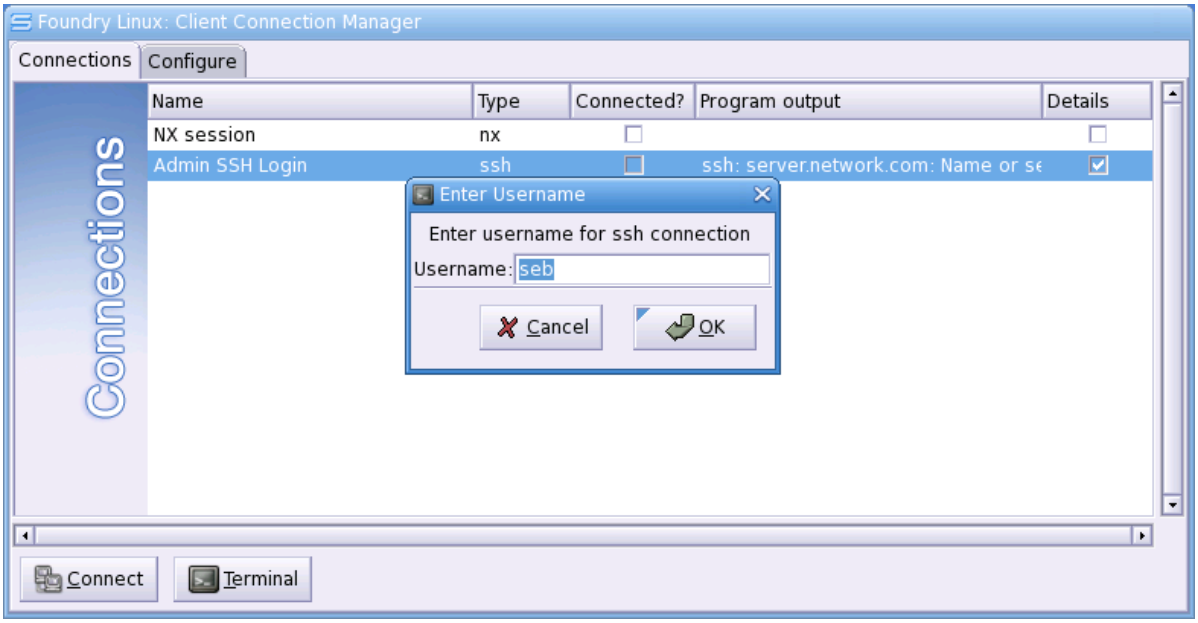


Illustration 33: Entering the ssh username on launching a connection

Copyright © 2008 William Matthew Limited. All rights reserved

Telnet

Configuring telnet sessions is almost identical to configuring an SSH connection. The only difference is that the username field is always ignored and the default port is 23.

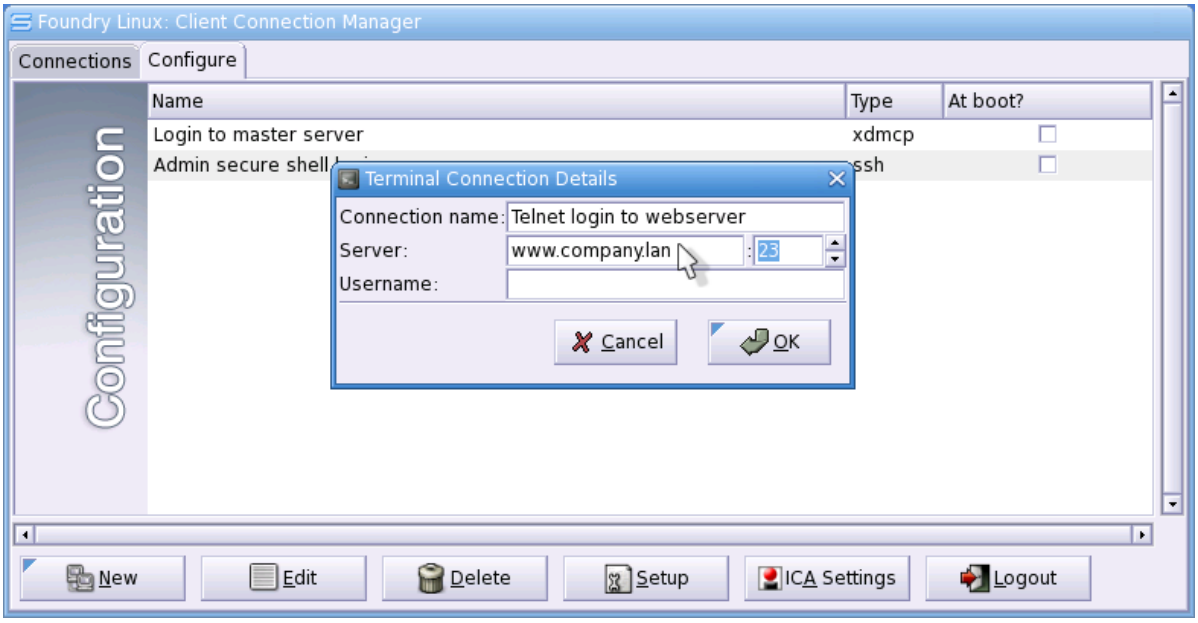


Illustration 34: Editing connections details for a telnet connection

Copyright © 2008 William Matthew Limited. All rights reserved

Web Browser

The WML Linux Thin Client ships with Mozilla Firefox.

To configure a web browser connection, click “New” in the Configuration tab, and select “web browser (mozilla)”.

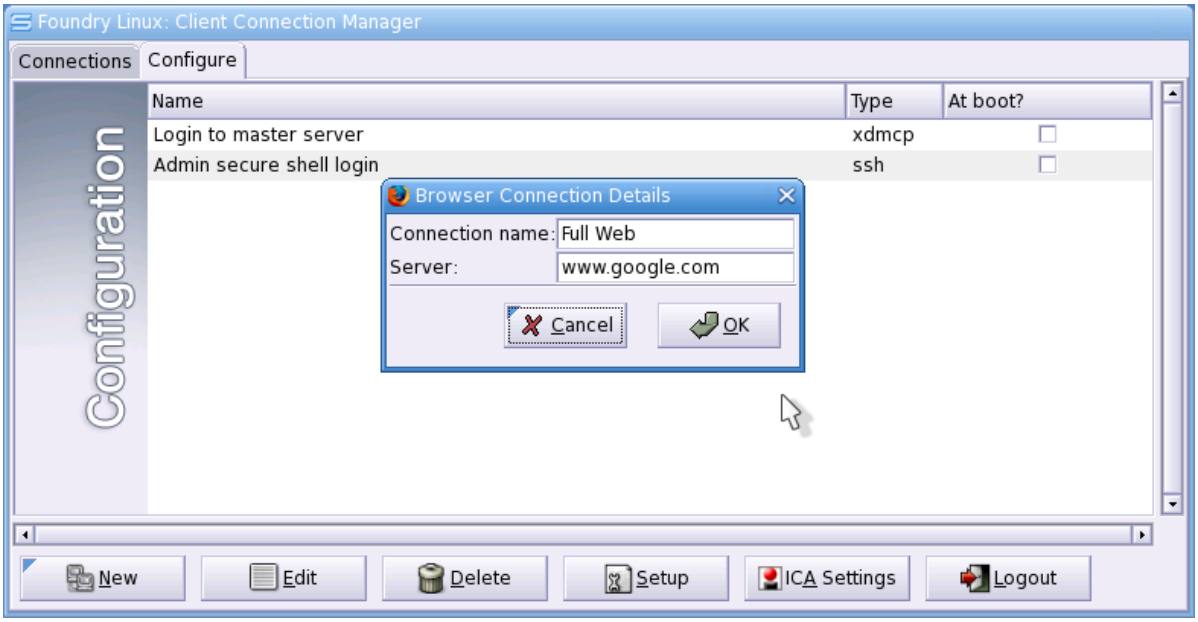


Illustration 35: Editing connection details for a web browser

There are only two fields to fill in, the connection name and the “Server”, which in this case is likely to be a normal website address.

Firefox settings

Firefox application settings are stored on the WML Linux Thin Client in an archive and unpacked into a ramdisk freshly, each time the browser launches. This means that bookmarks, saved passwords and other settings don't get stored on the thin client. It also ensures that one user cannot render the browser useless for the next user.

The system administrator can generate a site-specific set of Firefox settings. To do this first open the Mozilla Firefox browser and configure it suitably, then close the browser down. Next carry out the following command in a terminal window:

```
tar -cf /etc/persistent/firefox.tar -C /tmp/mozilla/ firefox
```

Illustration 36 shows the command being executed in a terminal window on the client.

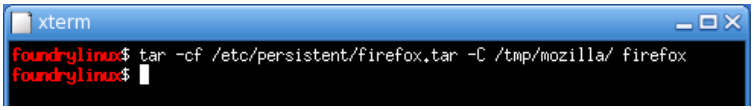


Illustration 36: Storing Mozilla Firefox settings from the last browser session

The configured settings will now be used each time Firefox is launched.

Copyright © 2008 William Matthew Limited. All rights reserved

Custom programs

The WML Linux Thin Client can be configured to run a local native binary program. Please contact WML for more information about compiling custom software using our development environment.

The WML Linux Thin Client can optionally provide the Mono execution environment to run .NET 1.1 programs. See www.go-mono.com for more details about Mono.

The WML Linux Thin Client provides both the Winforms library to run unmodified .NET 1.1 Windows programs, and the GTK# library so that desktop programs can be run with the same look and feel as the Foundry Linux Connection Manager.

Create a new connection in the Connection Manager and choose connection type "Custom .NET program".

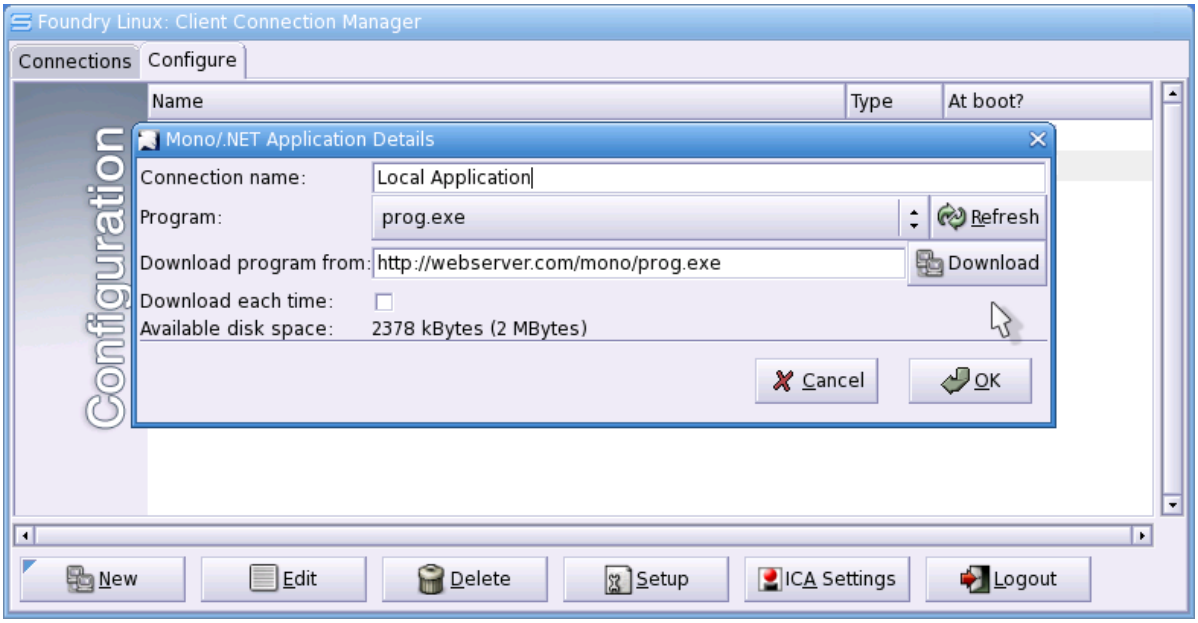


Illustration 37: Setting up a Mono .NET program to run locally on the WML Linux Thin Client

Enter the connection name for the program, as it will appear in the Connection Manager. *The name should match the title of the window which your program will create.* This is important, because the Connection Manager will recognise and manage your program's window based on its name. If the window doesn't match, the WML Linux Thin Client will be unable to switch from other connections to your program using the Ctrl-Alt-Down key combination.

The next field is a drop down menu, which will contain programs stored in the home directory of the WML Linux Thin Client user. If there is no program in this menu, then enter a URL to the program in the "Download program from" field and press the "Download" button. If the program downloads successfully, then it will appear in the "Program" drop down menu.

If you check "Download each time", then before running the program, the WML Linux Thin Client will try to download a fresh version of the program from the specified URL.

"Available disk space" tells you how much local storage is available to store the .NET program.

Copyright © 2008 William Matthew Limited. All rights reserved

Sun Secure Global Desktop

The WML Linux Thin Client provides the native Sun Secure Global Desktop client (previously known as Tarantella). Setup of Secure Global Desktop is simple:

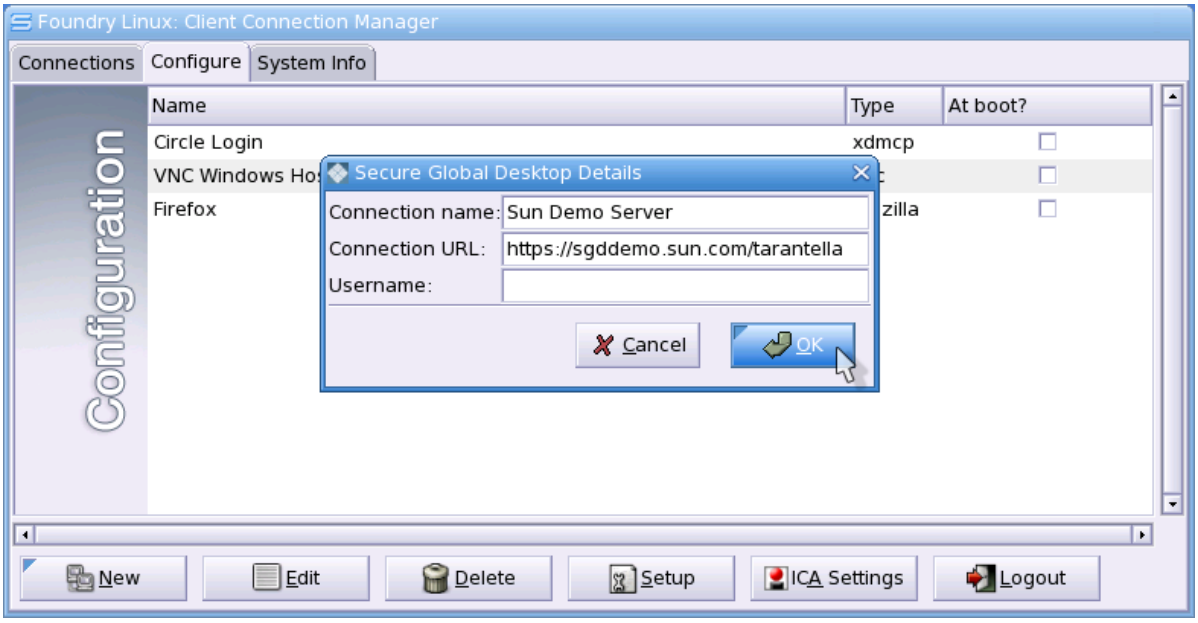


Illustration 38: Creating a new Sun Secure Global Desktop connection

Owners of clients with larger flash drives (128 MB andabove) are also able to access Secure Global Desktop using the Mozilla Firefox web browser and the Java plugin for Firefox.

Smartcards may be used with Secure Global Desktop for two factor authentications, using the optional Omnikey Cardman 3121.

Copyright © 2008 William Matthew Limited. All rights reserved

Client Setup Manager

The Setup Manager allows the system administrator to manage the WML Linux Thin Client's device settings. It allows you to control the network settings, the language/keyboard settings, display resolution, mouse settings, administrator password and sound.

The Setup Manager is also used to apply new firmware updates to the WML Linux Thin Client.

The Setup Manager can always be run by pressing the F2 key. It is password protected using the same password used to access the "Configuration" tab of the Connection Manager and has the default value of "password" on a factory delivered unit.

The Setup Manager is a tabbed window, with a tab for each section of the program.

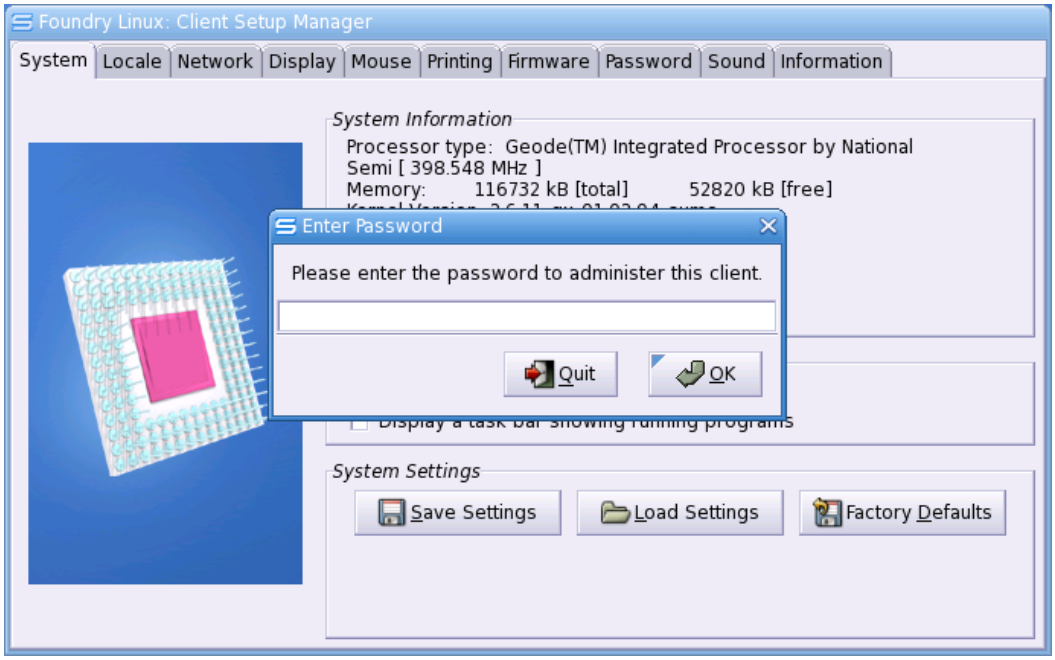


Illustration 39: The Setup Manager requests a password after it is launched with the F2 key.

Copyright © 2008 William Matthew Limited. All rights reserved

System

The System tab shows details about the thin client hardware and firmware.

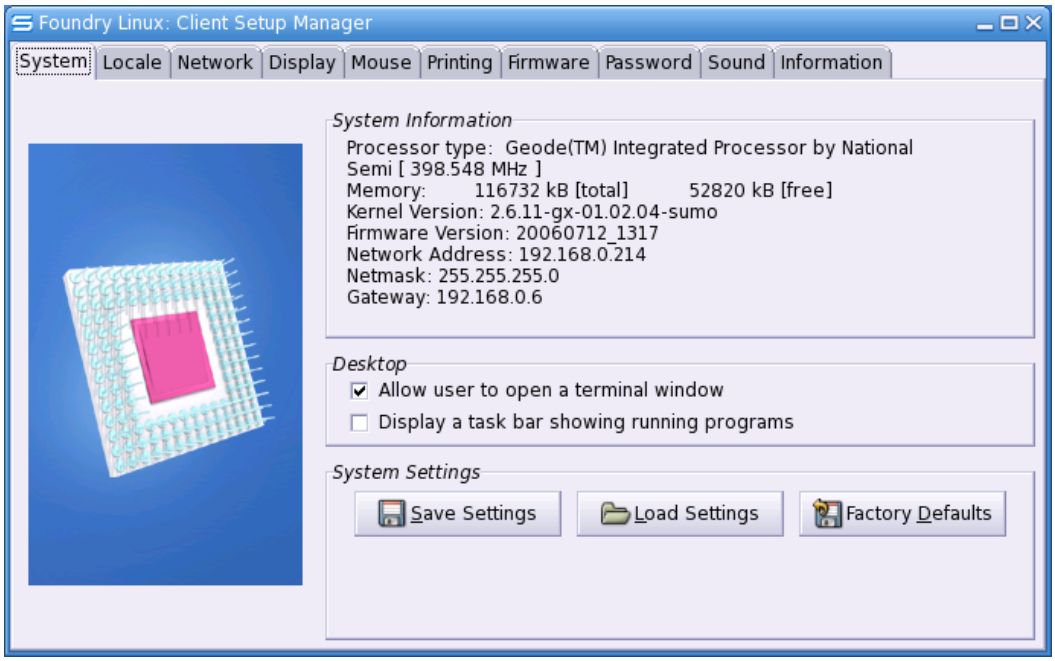


Illustration 40: The System Tab of the Setup Manager

The "System Information" box shows information about the processor type, the amount of memory available, the Linux kernel version and the Firmware version. The network settings are also shown in this box.

The "Desktop" box has two fields to control the thin client's desktop. The first check box controls whether a user may launch a command line terminal. If it is checked, a button will appear on the "Connections" tab of the Connection Manager called "Terminal".

Note that if a user has access to a terminal window, then it is possible for the user to modify the list of connections in the Connection Manager. Access to the terminal is intended for administrator and power users.

The second check box enables a task bar at the bottom of the screen which allows the user to navigate between windows.

Saving and Loading System Settings

The "System Settings" window has three buttons to help manage the WML Linux Thin Client. "Save Settings" will store the current system and connection configuration to a backup file, which is either stored on a usb storage device (if present) or in the temporary directory /tmp if not. "Save Settings" will save network, display, mouse, locale and password settings, as well as any connections which have been configured in the Connection Manager. The settings are saved in a file settings.tar.

Copyright © 2008 William Matthew Limited. All rights reserved

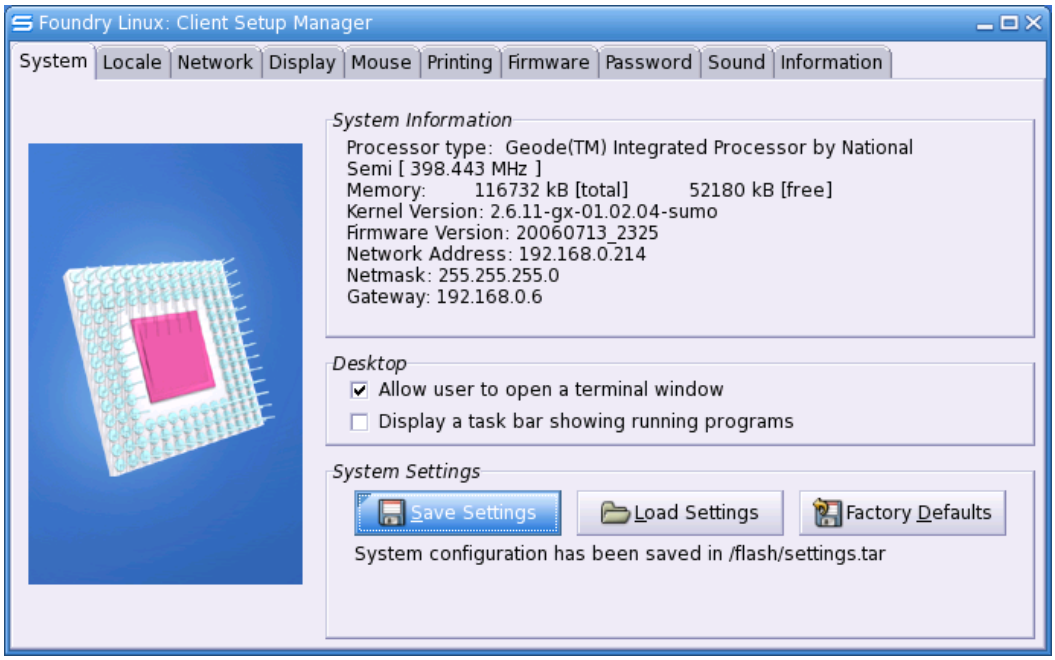


Illustration 41: Save Settings clicked, and settings saved on a usb storage device

To replicate a WML Linux Thin Client, take the usb storage device containing settings.tar and plug it into a new client. Press the "Load Settings" button. A file chooser dialog will appear, showing the contents of the /flash directory (the contents of the usb storage device).

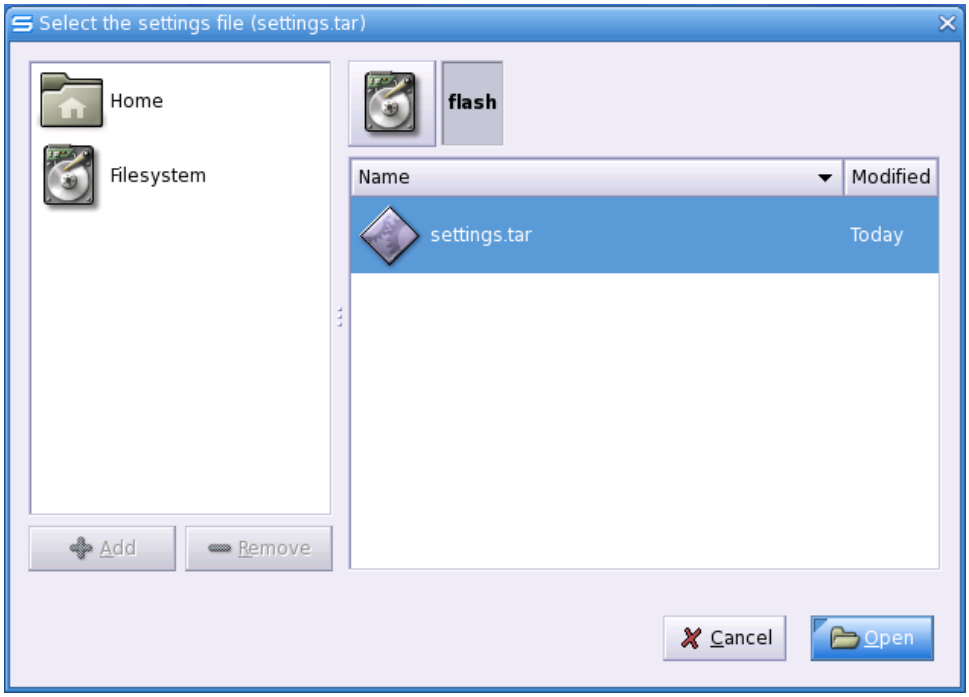


Illustration 42: Loading the settings file

Highlight the settings.tar file and press "Open". A confirmation box will open, asking you if you are sure and notifying you that the WML Linux Thin Client will re-boot if you confirm.

Copyright © 2008 William Matthew Limited. All rights reserved

Restoring Factory Default Settings

If you press the “Factory Defaults” button, a confirmation box will appear asking you to confirm that you wish to clear all configured connections and return the device to the factory default settings. This will reset all settings, including the administration password, and reboot the device. When the device powers up, the Setup Wizard will run.

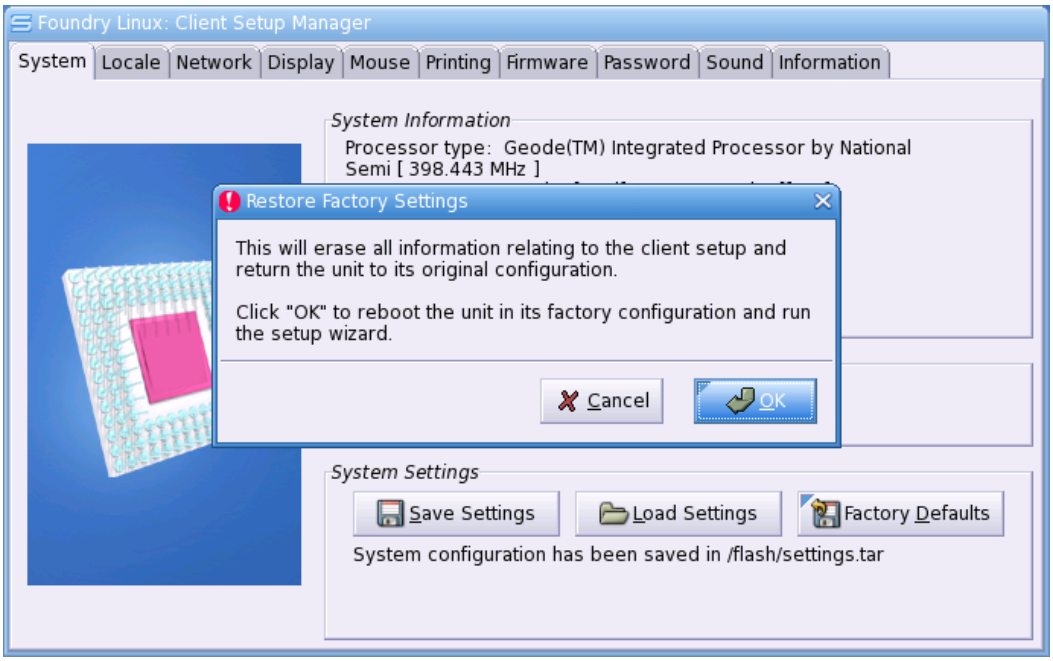


Illustration 43: Confirming Factory Default Settings

Network-wide configuration

The WML Linux Thin Client may be remotely configured using the saved file, settings.tar. It achieves this using DHCP (Dynamic Host Configuration Protocol). If the WML Linux Thin Client boots on a network with DHCP and the “next_server” DHCP parameter is specified, it will try to download a file from a web server whose address can be specified using the “next_server” DHCP parameter.

If “next_server” is specified as , for example, 192.168.0.1, then it will try to download http://192.168.0.1/foundrylinux/settings.tar If it is successful, it will apply these settings to the WML Linux Thin Client. If it can't download the file, startup will proceed as normal.

Note that the downloaded settings.tar should itself specify DHCP for network settings.

Copyright © 2008 William Matthew Limited. All rights reserved

Here is an example configuration directive for the Internet Systems Consortium DHCP Server, specifying the next_server parameter. This would be placed in the /etc/dhcp/dhcpd.conf file.

```
shared-network WORKSTATIONS {
    subnet 192.168.10.0 netmask 255.255.255.0 {
     range 192.168.10.100 192.168.10.150;
    }
     option subnet-mask            255.255.255.0;
     option broadcast-address      192.168.10.255;
     option routers                192.168.10.1;
     option domain-name-servers    123.23.232.23;
     option domain-name            "company.lan";
     next-server                  192.168.10.1;
}
```

In this example, the WML Linux Thin Client will try to download settings.tar from http://192.168.10.1/foundrylinux/settings.tar

Copyright © 2008 William Matthew Limited. All rights reserved

Locale

The Language/Keyboard is changed by selecting the desired locale from the drop-down menu. If you choose a new locale, a confirmation box will appear, and if you confirm, then the windowing session will re-start using the new language and keyboard settings.

Make sure you close down any connections you have running before changing the locale, as any open connections will be killed when the windowing system is re-started.

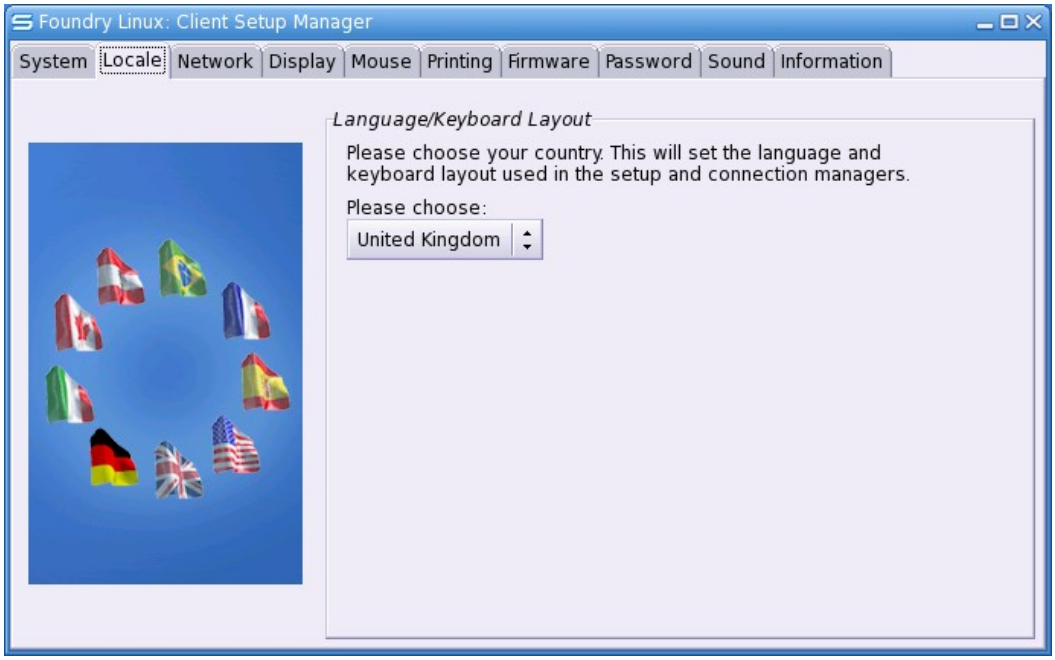


Illustration 44: The "Locale" tab of the Setup Manager

Copyright © 2008 William Matthew Limited. All rights reserved

Network

The WML Linux Thin Client's Network settings are configured using this tab. The WML Linux Thin Client can use DHCP to obtain its IP address and DNS settings, or these can be manually configured.

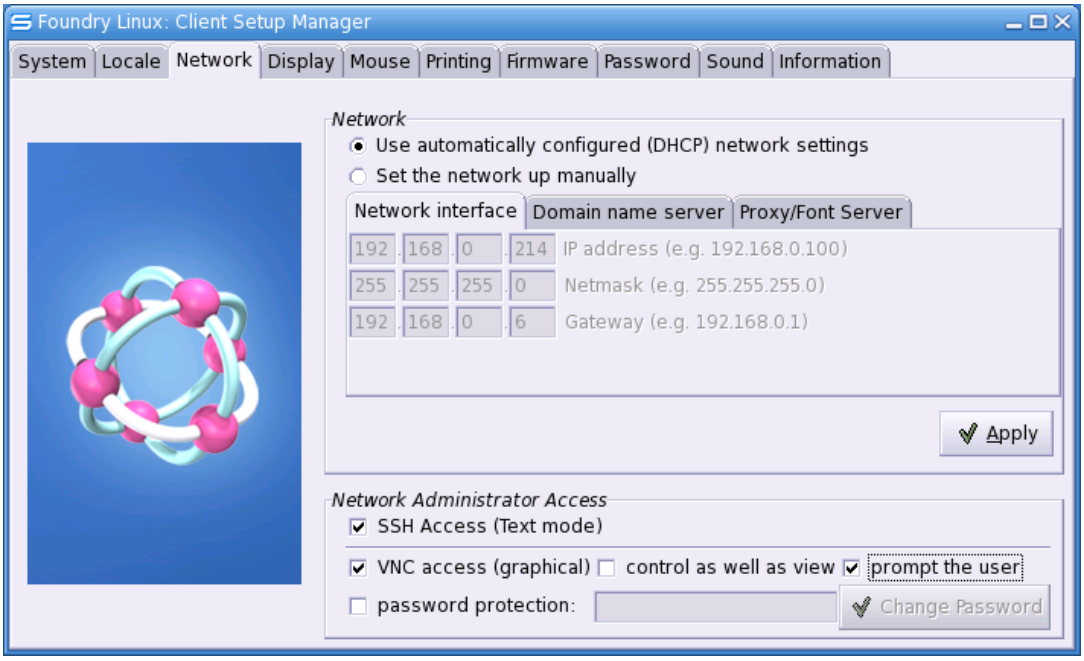


Illustration 45: Network settings set to DHCP

If the network settings are entered manually, details for IP address, netmask, gateway and name resolution need to be entered in the “Network interface”and “Domain name server” tabs. In the “Domain name server” settings, two DNS servers may be specified, along with a domain search path, which should be a space separated list of the domains on your network to search.

Remote access to the WML Linux Thin Client

The WML Linux Thin Client can be remotely accessed by an administrator either via secure shell, or using VNC. Both of these features need to be switched on in the Network tab of the Setup Manager. Illustration 45 shows both secure shell and VNC access switched on. The SSH and VNC daemons are started as soon as their respective boxes arechecked, the “Apply” button in the Network box needn't be pressed.

Remote SSH access

Secure shell provides a text based connection to the WML Linux Thin Client, which the admin can use to check memory usage and runaway processes.

Connect to the WML Linux Thin Client using any SSH client (for example, OpenSSH for unix, or Putty for Windows). Use the username “root” and the same password that you use to configure the WML Linux Thin Client.

Copyright © 2008 William Matthew Limited. All rights reserved

Remote VNC access

VNC provides a full graphical view of the WML Linux Thin Client's desktop. A number of options are provided:

"control as well as view" When checked, the remote admin will be able to control the desktop of the WML Linux Thin Client user, as well as viewing it.

"prompt the user" When this option is checked, the local WML Linux Thin Client user will see a pop-up window whenever a remote admin tries to view or control the desktop. The local user may then either refuse or accept the connection.

"password protection" Use a password to protect accessto the WML Linux Thin Client desktop. This password is stored separately fromthe usual admin password.

Specifying X Font Server (xfs)

The "Proxy/Font Server" tab allows the administrator to specify an X Font Server from which the WML Linux Thin Client should obtain font information. The WML Linux Thin Client runs its own font server, but this provides a very limited range of fonts. The Bitstream Vera truetype font is provided, along with a simple fixed X font. To allow tunnelled X applications to use a full range of fonts, a networked X font server can be used. Fill in the field with a suitable font server entry, and press "Set Font Server". An example is xfs.company.lan:7100

The default for the font server field is the local font server, unix/:7100. This font server remains in use, even when an additional font server is specified.

Currently, the proxy configuration setting is made within the web browser, rather than in the Setup Manager.

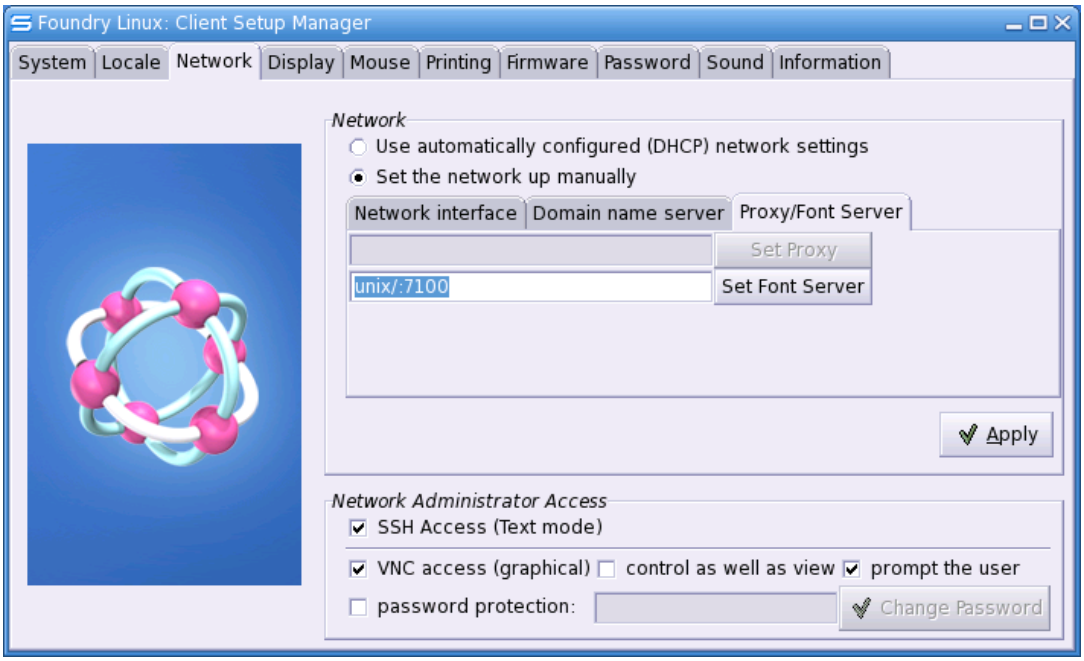


Illustration 46: Highlighting the x font server field to specify an additional font server.

Copyright © 2008 William Matthew Limited. All rights reserved

Wireless networking

Currently, wireless networking must be configured by editing text configuration files. Wireless networking can be achieved on the WML Linux Thin Client GX using a plugin usb wireless device based on the prism2 chipset. The WML Linux Thin Client LX can be supplied with an optional Intel Pro2200b/g or Atheros wireless card. In each case, the wireless device is configured in the file /etc/persistent/prestartup.sh.

To edit prestartup.sh, you must get a root shell on the WML Linux Thin Client. You can either press Ctrl-Alt-F1 to get a login prompt, then login as "root" with the usual admin password used to gain access to the Setup Manager. Alternatively, if you have sshd running for remote admin, you can ssh to your WML Linux Thin Client (to ssh to your own WML Linux Thin Client, type: ssh root@localhost).

Now edit the prestartup.sh file:

```
nano -w /etc/persistent/prestartup.sh
```

And modify the commented out commands. The first commands load the kernel modules to drive the wireless device. The next group of commands use either wlanctl-ng (prism2) or iwconfig (intel pro2200 and atheros) to configure the SSID and WEP or WPA-PSK settings for the device.

```
#!/bin/sh
# This script is executed at startup before the network interfaces are
# configured. It's the right place to configure wireless devices.
#
# Example 1: setting up integrated minipci Atheros wireless network card
#
################################################################################
#
## Load 3 modules for the integrated minipci Atheros wireless network card
## (madwifi 0.9.4):
modprobe wlan_scan_sta
modprobe ath_rate_sample
modprobe ath_pci
#
## If you need WEP, then add the wep module
modprobe wlan_wep
## If you need WPA then add these two modules:
#modprobe wlan_tkip
#modprobe wlan_ccmp
#
## This module uses wireless-tools (iwconfig etc) for controlling settings
#
## Set up wireless interface. Here the SSID is set to join a managed wlan
## called HYPERCUBE.
iwconfig ath0 essid HYPERCUBE >/dev/null 2>&1
## If your SSID has spaces in, then place the SSID in double quotes:
#iwconfig ath0 essid "HYPER CUBE" >/dev/null 2>&1
#
## If you want to use WEP, set the key like this for your ascii key.
## (Don't forget to modprobe wlan_wep, above)
#iwconfig ath0 key s:asciikey
## or for a hex key like this:
iwconfig ath0 key 1a1a1a1a1a
#
## If you want to use WPA-PSK, then uncomment this line, and edit
```


Copyright © 2008 William Matthew Limited. All rights reserved

```
## /etc/persistent/wpa_supplicant.conf with your ssid and
## WPA-PSK passphrase. We find the pause here is necessary with the
## Atheros wireless device.
#wpa_supplicant -B -Dwext -iath0 -c/etc/persistent/wpa_supplicant.conf
#echo "Wireless: Associating with wireless access point..."
#sleep 15
#
## Bring up the interface (i.e. switch on the radio)
ifconfig ath0 up
## Apply a timeout to allow Atheros chip to find correct wireless frequency
## and especially if you use dhcp to obtain an IP address.
echo "Wireless: Waiting for IP address..."
sleep 15
## Network settings can now be made for ath0 by manually editing
## /etc/interfaces (use the nano editor)
```

This example was created by taking the default prestartup.sh, and un-commenting the lines for a WEP based wireless network. You can always get the original example prestartup.sh file by extracting it from the default settings archive:

```
cd /tmp && tar xvf /usr/persist.tar prestartup.sh
```

will extract prestartup.sh into the /tmp directory

If you want to use WPA-PSK, rather than WEP, then comment the line "iwconfig ath0 key 1a1a1a1a1a" and un-comment the wpa_supplicant line. You will then need to edit /etc/persistent/wpa_supplicant.conf so that it looks something like this:

```
# This is a configuration file for the program wpa_supplicant.
# You can find further configuration options in the wpa_supplicant
# documentation, which can be found online.
network={
ssid="YOUR_SSID"
proto=WPA
key_mgmt=WPA-PSK
# Either use the passphrase un-hashed:
psk="Your_passphrase"
# or use the hash generated with:
# wpa_passphrase "YOUR_SSID" "Your_passphrase":
#psk=c2cc546a4b526622eae137106dff9a24e46591d01fabf7429e9623a54fc0f
9cf
}
```

You may need to experiment with the number value for the "sleep 15" call (which means pause for 15 seconds).

Once the prestartup.sh file has been configured correctly, you will need to manually amend the /etc/persistent/interfaces file. An example of a dhcp configured system with an Atheros network interface is:

```
auto lo ath0
iface lo inet loopback
iface ath0 inet dhcp
```


Copyright © 2008 William Matthew Limited. All rights reserved

The equivalent for the Intel Pro Wireless card would be:

```
auto lo eth1
iface lo inet loopback
iface eth1 inet dhcp
```

Note that the only difference is the way the Linux kernel refers to the wireless device; theAtheros is “ath0” and the Intel is “eth1”.

To configure the IP address settings statically, edit /etc/persistent/interfaces to look something like this:

```
auto lo ath0
iface lo inet loopback
iface ath0 inet static
     address 192.168.0.10
     netmask 255.255.255.0
     gateway 192.168.0.1
```


Copyright © 2008 William Matthew Limited. All rights reserved

Display

The display resolution tab presents a menu of supported resolutions and refresh rates. These are determined from your monitor using a DDC query.

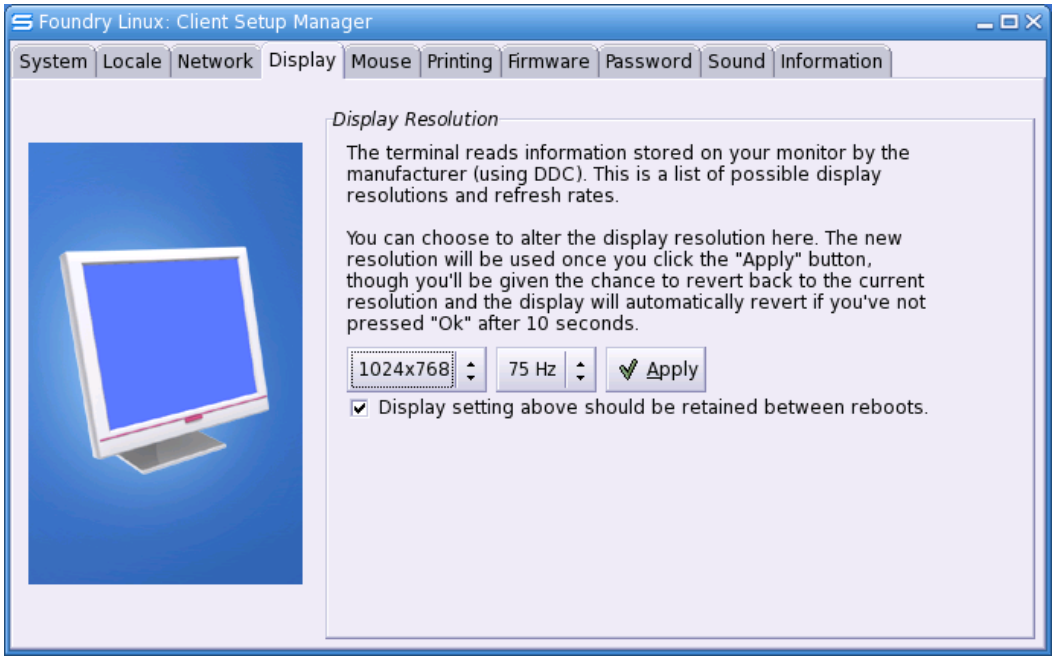

Foundry Linux: Client Setup Manager
System
Locale
Network
Display
Mouse
Printing
Firmware
Password
Sound
Information
Display Resolution
The terminal reads information stored on your monitor by the manufacturer (using DDC). This is a list of possible display resolutions and refresh rates.
You can choose to alter the display resolution here. The new resolution will be used once you click the "Apply" button, though you'll be given the chance to revert back to the current resolution and the display will automatically revert if you've not pressed "Ok" after 10 seconds.
1024x768
75 Hz
Apply
Display setting above should be retained between reboots.

Illustration 47: The "Display" tab of the Setup Manager

If you wish to change the display resolution, choose the new setting and click “Apply”. If the box is checked (“Display settings above should be retained between reboots”), then the next time the WML Linux Thin Client boots, it will *not* automatically detect the optimum monitor resolution but will run your chosen resolution.

If you want to return the WML Linux Thin Client to checking automatically for resolution, simply uncheck the box. This can be useful when preparing a settings.tar file to implement remote management for a fleet of clients.

Copyright © 2008 William Matthew Limited. All rights reserved

Mouse

The mouse settings tab allows the mouse speed and handedness to be configured.

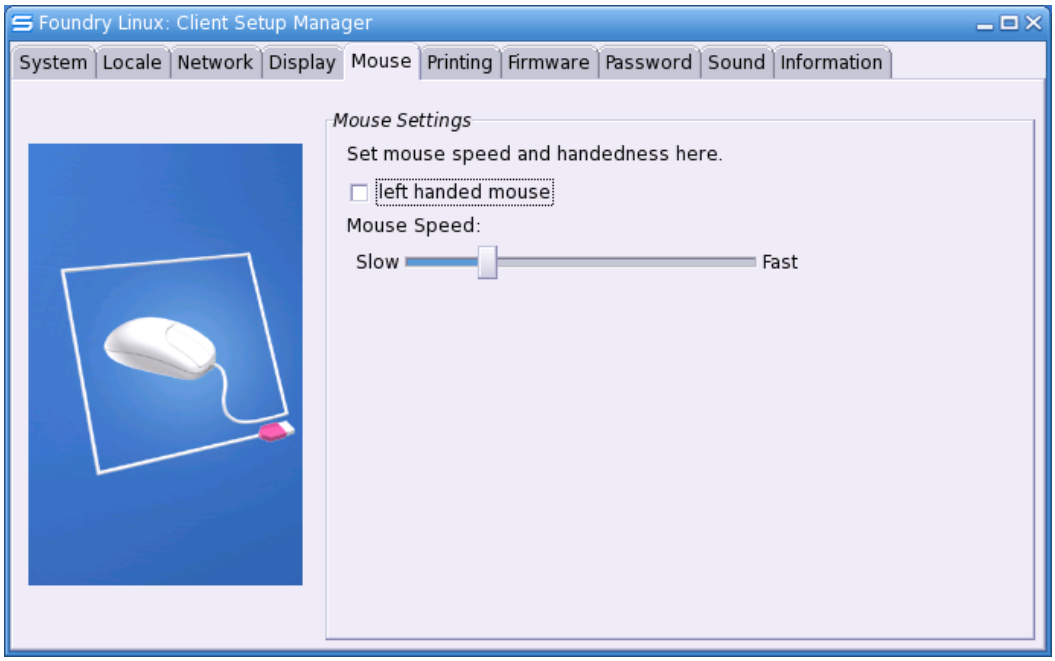


Illustration 48: Mouse set to the default speed and right-handed operation.

Copyright © 2008 William Matthew Limited. All rights reserved

Printing

The printing tab provides some information about printing via the WML Linux Thin Client. On devices with a parallel port, a menu is provided to choose whether theprinter is attached to the parallel or usb port. On the standard WML Linux Thin Client, only usb ports are available.

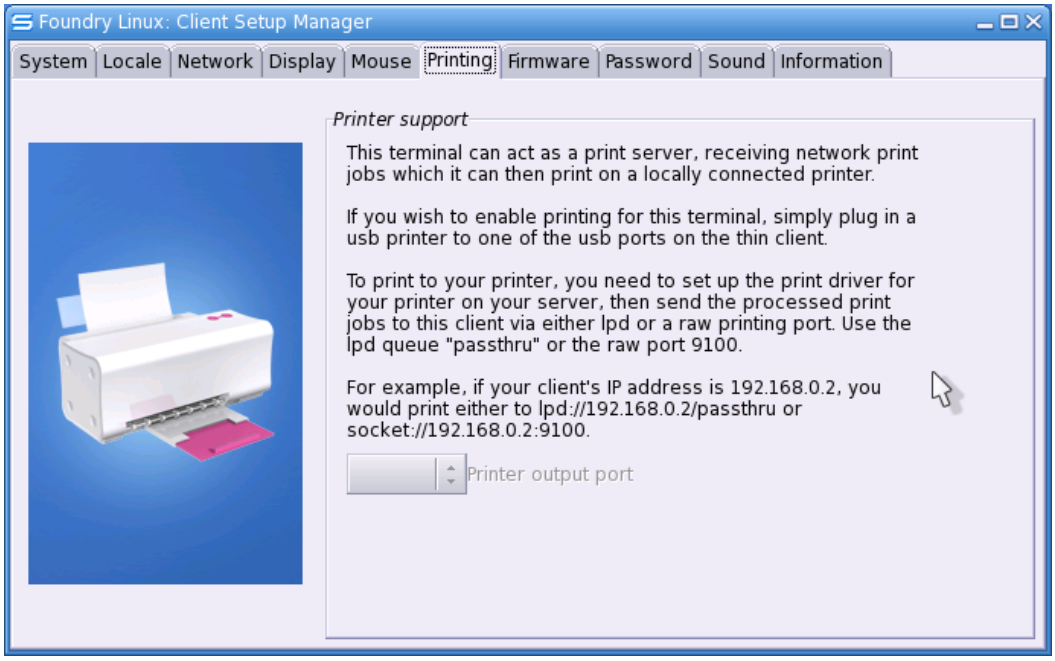

Foundry Linux: Client Setup Manager
System
Locale
Network
Display
Mouse
Printing
Firmware
Password
Sound
Information
Printer support
This terminal can act as a print server, receiving network print jobs which it can then print on a locally connected printer.
If you wish to enable printing for this terminal, simply plug in a usb printer to one of the usb ports on the thin client.
To print to your printer, you need to set up the print driver for your printer on your server, then send the processed print jobs to this client via either lpd or a raw printing port. Use the lpd queue "passthru" or the raw port 9100.
For example, if your client's IP address is 192.168.0.2, you would print either to lpd://192.168.0.2/passthru or socket://192.168.0.2:9100.
Printer output port

Illustration 49: Printer support information

Copyright © 2008 William Matthew Limited. All rights reserved

Firmware

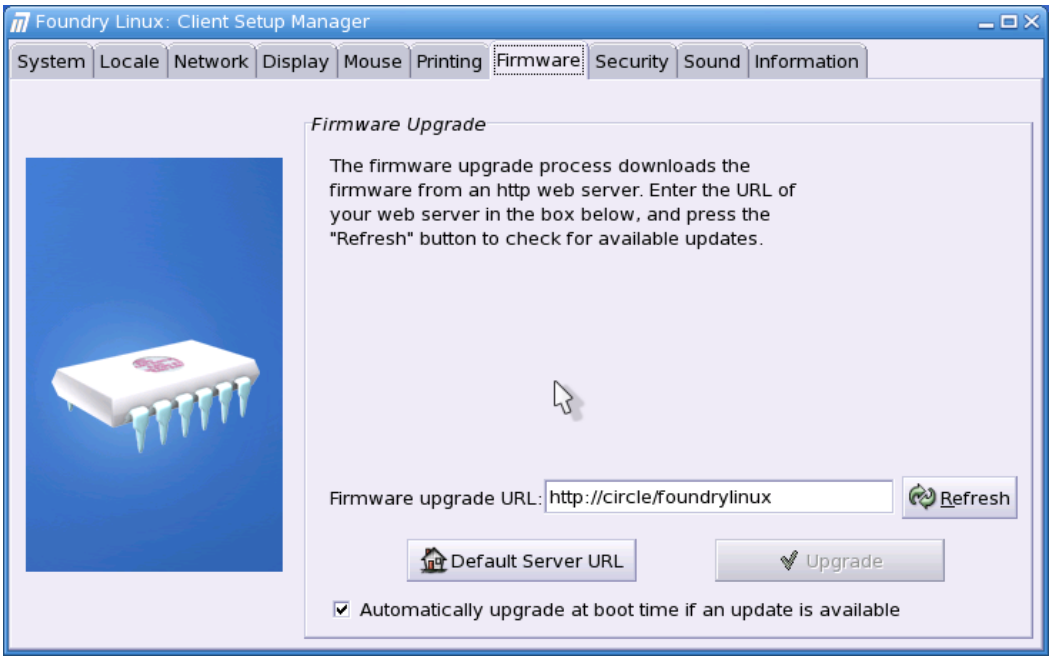
Firmware upgrades are performed over the network. The WML Linux Thin Client downloads firmware image files from a specified web server and copies them onto its internal flash storage before rebooting. The upgrades can be performed manually, only when the admin wishes to apply a new firmware, or automatically at boot time, as soon as a new image becomes available.

Firmware image files are available from William Matthew Limited's web servers. The firmware files can be copied to your own webserver for faster upgrades on a corporate network.

Manually Initiating a Firmware Upgrade

Illustration 50 shows the Firmware upgrade tab in its initial state. There is a "Refresh" button, which will check for a new firmware at the Firmware upgrade URL, a "Default Server URL" button, which will restore the Firmware upgrade URL to the default of "http://wmltd.co.uk/foundrylinux" and a checkbox to specify whether the unit should automatically upgrade if a new image is available at the Firmware upgrade URL.

Illustration 50: The Firmware Upgrade tab



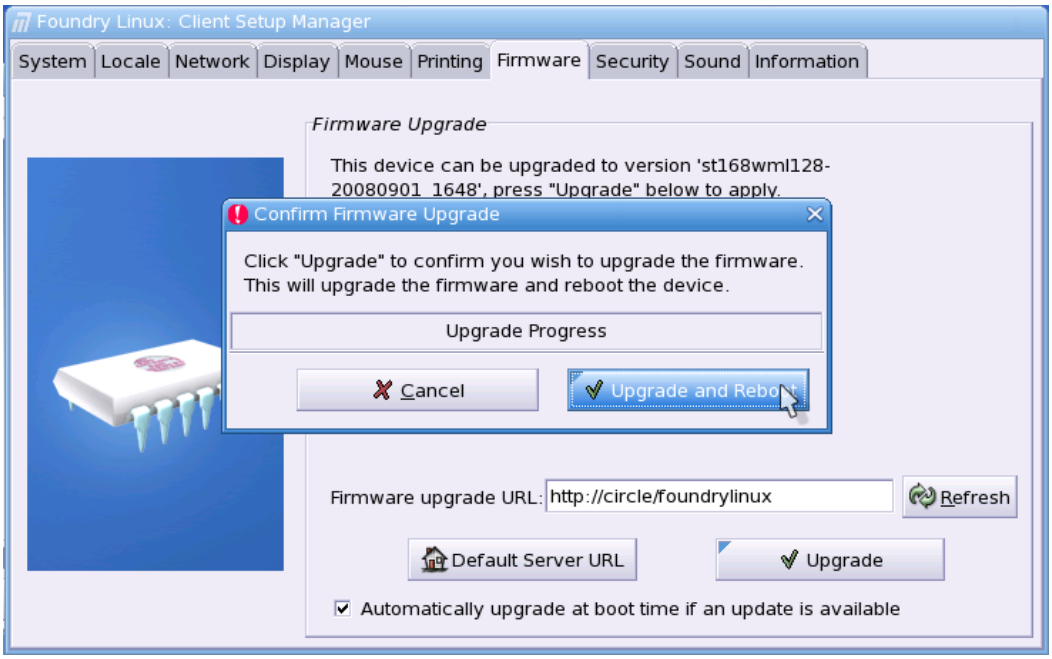
After pressing Refresh, the tab will tell you if a firmware is available, and if so, whether your unit is up to date, or can be updated.

If a new firmware is available, then the "Upgrade" button will be un-greyed, and on pressing it, a confirmation window will show, where you can "Upgrade and Reboot" or cancel the upgrade.

Do not interrupt the upgrade process once it is underway, or power off the device. The process will take a few minutes, mainly determined by the speed of the network connection between the Linux Thin Client and the web server.

Copyright © 2008 William Matthew Limited. All rights reserved

Illustration 51: Confirming the Firmware Upgrade



Upgrading the firmware will not change the device settings or affect the configured connections in the Connection Manager.

Automatic Firmware Upgrades

If the unit has been configured to automatically upgrade, as shown in Illustration 51 (the checkbox is checked), then at boot time, the Linux Thin Client will check the URL for an update and the proceed to upgrade and reboot if necessary. During the upgrade, a progress window will show, then the unit will reboot and run the Connection Manager as normal.

Copyright © 2008 William Matthew Limited. All rights reserved

Automatic Firmware Update
Firmware Upgrade
The firmware on this device is being automatically upgraded.
The device will reboot when the upgrade is complete.
Root filesystem downloaded successfully...

Illustration 52: Automatic firmware upgrade progress window

Installing a firmware upgrade file on a LAN web server

In corporate networks, it is advisable to change the Firmware upgrade URL from the default WML web server in order to take control of firmware upgrades. A new upgrade can be tested on a sample unit before being rolled out across the organisation.

The firmware image is around 40 megabytes in size and will take some time to upgrade over a regular broadband internet connection, providing a further reason to install the firmware upgrade on a LAN server.

Firmware upgrade images are distributed as a gzipped tar archive containing several files. The latest image is always available at http://wmltd.co.uk/foundrylinux/. At the time of writing, the most recent firmware is: st168wml128-20080820_1233.tar.gz. http://wmltd.co.uk/foundrylinux always contains both the archive file and the contents of the archive file.

This archive contains the following files:

- boot.tar
- boot.tar.md5
- persist.tar
- persist.tar.md5
- preupdate.sh
- preupdate.sh.md5
- rootfs.img
- rootfs.img.md5
- version.txt

All of these files should be available from the Firmware upgrade URL – the thin client downloads the files separately, rather than downloading and untarring the archive file itself.

Copyright © 2008 William Matthew Limited. All rights reserved

For example, if you intend to set the Firmware upgrade URL to "http://mycorp.lan/foundrylinux" and on mycorp.lan, the foundrylinux directory is at /var/www/foundrylinux/ then you can run the following command to unpack st168wml128-20080820_1233.tar.gz into /var/www/foundrylinux/:

```
tar -xvzf /path/to/st168wml128-20080820_1233.tar.gz -C /var/www/foundrylinux/
```


Copyright © 2008 William Matthew Limited. All rights reserved

Password

The System administrator password can be changed using the Password tab of the Setup Manager. Enter the new password in the field and press “Change Password”. You will be asked to confirm the password by re-entering it. If the two passwords match, and are greater in length than 5 character, the password will be updated.

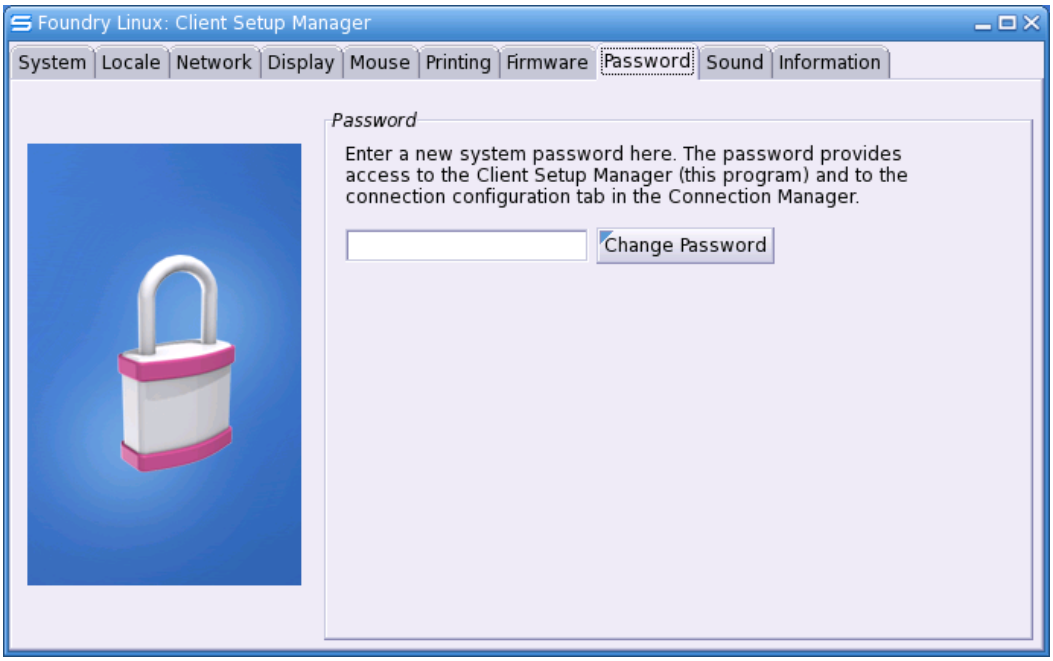


Illustration 53: Updating the administrator password

Copyright © 2008 William Matthew Limited. All rights reserved

Sound

The WML Linux Thin Client supports networked sound for ICA and Unix/Linux connection types. The sound tab allows you to start or stop the esound daemon. The esound daemon allows Unix sessions to support networked audio.

If you use sound for Citrix sesssions, the esound daemon must be switched off.

When you switch the esound daemon on, with speakers or headphones connected, you will hear a series of tones (best not to wear the headphones when doing this – the sounds may be quite loud).

To send audio from your Unix/Linux application to the WML Linux Thin Client, it is necessary to configure the application to send audio output to "esound" or "esd" rather than the usual ALSA or OSS. No other action need be taken. If you have difficulty configuring sound, please check the firewall settings on your application server; the esound daemon listens for TCP packets on port 16001.

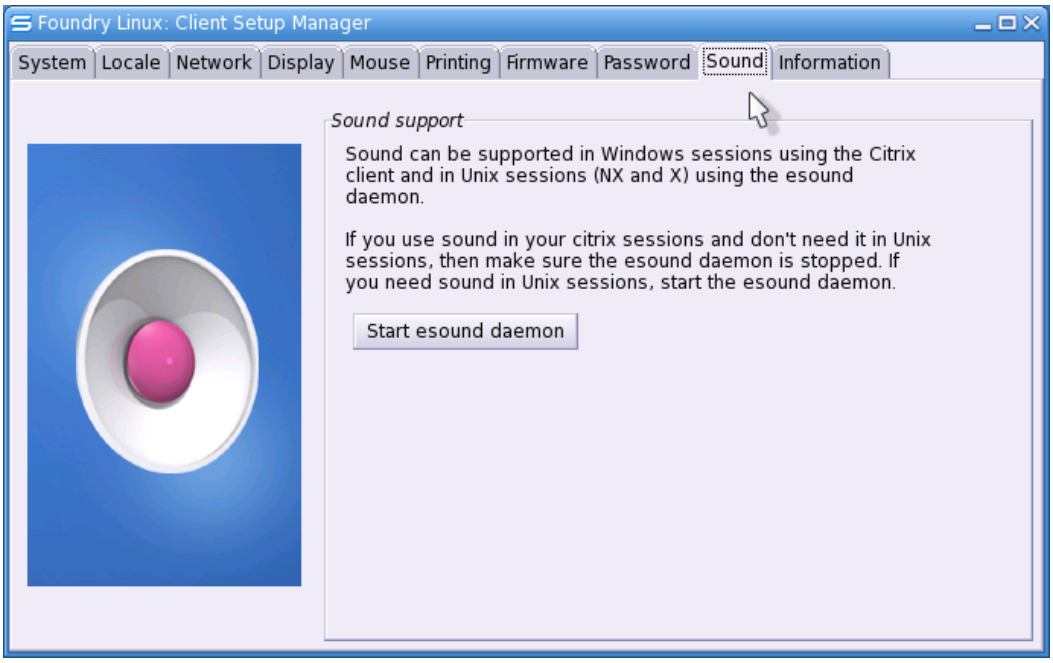

Foundry Linux: Client Setup Manager
System
Locale
Network
Display
Mouse
Printing
Firmware
Password
Sound
Information
Sound support
Sound can be supported in Windows sessions using the Citrix client and in Unix sessions (NX and X) using the esound daemon.
If you use sound in your citrix sessions and don't need it in Unix sessions, then make sure the esound daemon is stopped. If you need sound in Unix sessions, start the esound daemon.
Start esound daemon

Illustration 54: Switching on the esound daemon

Copyright © 2008 William Matthew Limited. All rights reserved

Information

This tab presents Copyright information for the Connection Manager, the Setup Manager and free software included with the WML Linux Thin Client.

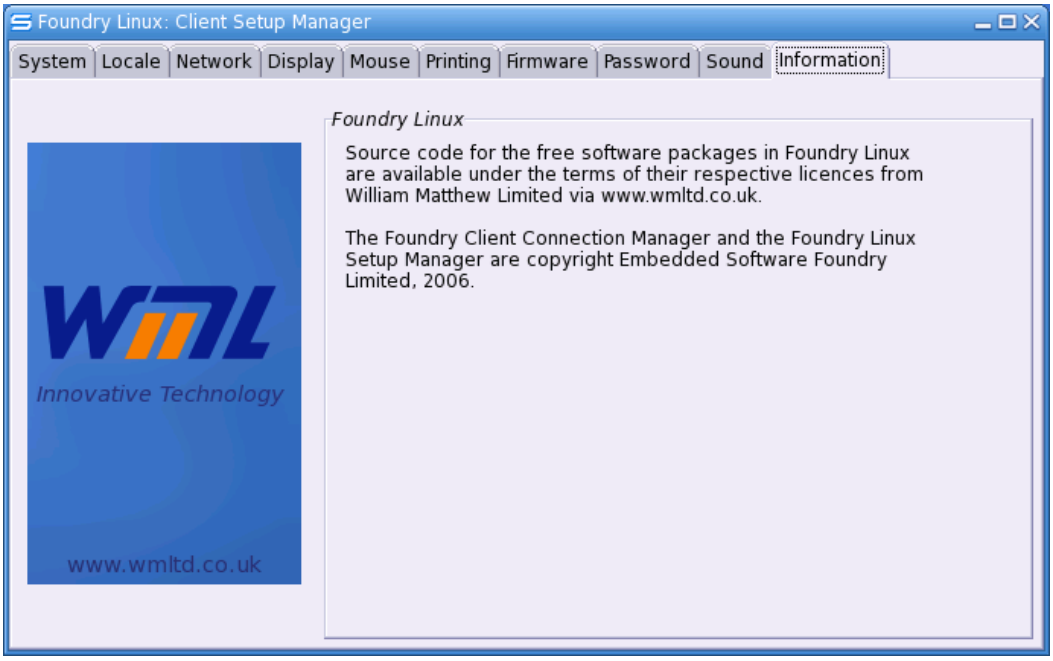


Illustration 55: Copyright information

Copyright © 2008 William Matthew Limited. All rights reserved

Administrator and Power User Tools

The WML Linux Thin Client bundles a few programs which system administrators and power users will find useful. These are available from the command line, which can be accessed by checking the "allow user to open a terminal" checkbox on the "System" tab of the Setup Manager. A "Terminal" button will appear in the Connection Manager

Using the terminal, telnet and ssh connections may be made with the full range of options available. Power users may also wish to make rdesktop RDP connections or vncviewer connections using the command line, but note that these connections will not be managed, and can't be switched between using the Ctrl-Alt-Down key combination.

The WML Linux Thin Client comes with a very simple vi editor, and the more useful GNU Nano text editor. Nano can be launched using either the "nano" command, or its alias "edit".

Files can be transferred using scp (secure copy – part of the openssh toolkit) or sftp. Files may be downloaded using wget.

Startup script

The WML Linux Thin Client may be controlled using an optional startup script. This script is executed after all kernel modules have been installed, and after the network has been configured. It can be used to configure a wireless network card or set up NFS network mounts or indeed, anything that may be necessary to prepare the WML Linux Thin Client to work on your network, or support your embedded Mono/.NET applications.

There are TWO startup scripts; /etc/persistent/prestartup.sh, which executes BEFORE the network has been configured (and is thus the correct location for setting up wireless modules) and /etc/persistent/startup.sh which is executed after the network has been configured.

To add a script, edit a file called /etc/persistent/startup.sh and make it executable:

```
edit /etc/persistent/startup.sh
```

Add lines; the script is a busybox shell script:

```
#!/bin/sh
# Comments start with a # character
/bin/echo "test file" > /etc/persistent/output.txt
```

Now make it executable:

```
chmod a+x /etc/persistent/startup.sh
```

The script will now be executed every time the WML Linux Thin Client boots.

Copyright © 2008 William Matthew Limited. All rights reserved

Smartcard support

The WML Linux Thin Client can optionally support the Omnikey 3120 usb smartcard reader. The pcscd program will run when a smartcard is connected, which will provide networked access to the smartcard data. pcscd is the daemon program for the industry standard pcsc-lite and musclecard framework. pcscd provides a smartcard device independent method of accessing data on the smartcard.

For more information about implementing smartcard support, please contact William Matthew Limited.

Copyright © 2008 William Matthew Limited. All rights reserved